2013-03

Analysis of the United States Computer Emergency Readiness Team's (U.S. CERT) Einstein III intrusion detection system, and its impact on privacy

Oree, William L.

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

ANALYSIS OF THE UNITED STATES COMPUTER EMERGENCY READINESS TEAM'S (U.S. CERT) EINSTEIN III INTRUSION DETECTION SYSTEM, AND ITS IMPACT ON PRIVACY

by

William L. Oree

March 2013

Thesis Advisor: Glenn Cook
Second Reader: John Fulp

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704–0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202–4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704–0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** March 2013	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Analysis of the United States Computer Emergency Readiness Team's (U.S. CERT) Einstein III intrusion detection system, and its impact on privacy		**5. FUNDING NUMBERS**	
6. AUTHOR(S) William L. Oree			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943–5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number _____N/A_____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE**	

13. ABSTRACT (maximum 200 words)

To secure information technology and telecommunications systems, the U.S Department of Homeland Security created the United States Computer Emergency Readiness Team (U.S. CERT) to provide 24-hour early warning and detection for the federal government's Internet infrastructure. A leading program in this effort, EINSTEIN, was developed by U.S. CERT in partnership with the National Security Agency (NSA) and private industry. EINSTEIN is an intrusion detection program that monitors network traffic and searches for signatures of known malicious code. Now in its third generation, EINSTEIN now generates alerts that have the possibility of including Personal Identifying Information, monitors live traffic on networks in real-time, and also has the ability to counter the intrusion as it takes place.

By reviewing current privacy policy and past privacy case studies, in addition to careful analysis of federal court cases and statutes, this thesis establishes the fundamental and constitutional right to privacy. Through secondary research, this thesis identifies elements and exemptions of current communications legislation that can be used in the development of a comprehensive cyberspace monitoring policy. The result is a recommendation that a new Einstein III Privacy Impact Assessment, as well a new legal opinion document, be drafted to balance the trade-off between privacy rights and the objectives of securing cyberspace, and that establishes a proper legal foundation for the implementation of the controversial technology.

14. SUBJECT TERMS EINSTEIN, Intrusion Detection System, Cybersecurity, Privacy			**15. NUMBER OF PAGES** 97
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540–01–280–5500 Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

ANALYSIS OF THE UNITED STATES COMPUTER EMERGENCY READINESS TEAM'S (U.S. CERT) EINSTEIN III INTRUSION DETECTION SYSTEM, AND ITS IMPACT ON PRIVACY

William L. Oree
Lieutenant, United States Navy
B.S., Armstrong Atlantic State University, 2004

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF SCIENCE IN
INFORMATION TECHNOLOGY MANAGEMENT**

from the

**NAVAL POSTGRADUATE SCHOOL
March 2013**

Author: William L. Oree

Approved by: Glenn Cook
Thesis Advisor

John Fulp
Second Reader

Dr. Dan Boger
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

To secure information technology and telecommunications systems, the U.S Department of Homeland Security created the United States Computer Emergency Readiness Team (U.S. CERT) to provide 24-hour early warning and detection for the federal government's Internet infrastructure. A leading program in this effort, EINSTEIN, was developed by U.S. CERT in partnership with the National Security Agency (NSA) and private industry. EINSTEIN is an intrusion detection program that monitors network traffic and searches for signatures of known malicious code. Now in its third generation, EINSTEIN now generates alerts that have the possibility of including Personal Identifying Information, monitors live traffic on networks in real-time, and also has the ability to counter the intrusion as it takes place.

By reviewing current privacy policy and past privacy case studies, in addition to careful analysis of federal court cases and statutes, this thesis establishes the fundamental and constitutional right to privacy. Through secondary research, this thesis identifies elements and exemptions of current communications legislation that can be used in the development of a comprehensive cyberspace monitoring policy. The result is a recommendation that a new Einstein III Privacy Impact Assessment, as well a new legal opinion document, be drafted to balance the trade-off between privacy rights and the objectives of securing cyberspace, and that establishes a proper legal foundation for the implementation of the controversial technology.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACLU	American Civil Liberties Union
APA	Administrative Procedure Act
CCPA	Cable Communications Policy Act
CDT	Center for Democracy & Technology
CHUI	Card Holder Unique Identifier
CIO	Chief Information Officer
CISPA	Cyber Intelligence Sharing and Protection Act
CNCI	Comprehensive National Cybersecurity Initiative
CS&C	Office of Cybersecurity and Communications
CRS	Congressional Research Service
CYBERCOM	United States Cyber Command
DBS	Direct Broadcast Satellite
DHS	Department of Homeland Security
DOJ	Department of Justice
DON	Department of the Navy
ECPA	Electronic Communications Privacy Act
EFF	Electronic Frontier Foundation
EPIC	Electronic Privacy Information Center
FBI	Federal Bureau of Investigations
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standard
FISA	Foreign Intelligence Surveillance Act
FISC	Federal Intelligence Surveillance Court
FCISC	Federal Cyberspace Intelligence Surveillance Court
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
HEW	Health Education and Welfare
HSPD	Homeland Security Presidential Directive
IDS	Intrusion Detection System
IRS	Internal Revenue Service

ISP	Internet Service Provider
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSL	National Security Letter
NSPD	National Security Presidential Directive
OMB	Office of Management and Budget
OPNAV	Chief of Naval Operations
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIV	Personal Identity Verification
RFID	Radio Frequency Identification
SECURE IT	Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act
SIGINT	Signals Intelligence
TICAP	Trusted Internet Connection Access Provider
U.S. CERT	United States Computer Emergency Readiness Team

ACKNOWLEDGMENTS

I wish to thank the instructors and staff of the Graduate School of Operational and Information Sciences for providing me with an enriching academic experience, and I would like to thank Glenn Cook and J. D. Fulp for guiding my research during the writing of this thesis.

I would like to give a special thanks to my two sons, Kenji and Syrus, and to my wonderful wife, Makiko, for being so supportive and understanding while I sacrificed time away from the family to complete this project. You have always been my greatest cheerleaders, and without your support I would never have been able to do this. Thank you for everything you do for me!

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

In the years following the terrorist attacks of 9/11 the Department of Homeland Security (DHS) was created to secure the nation from many threats. Among these threats, those of increasing significance were threats to the federal government's computer network infrastructure and the computer network infrastructure of private sector companies that do business with government agencies. To address this growing issue several policy documents have been written and government structures created. However, the cybersecurity system is not working, attacks against federal networks have increased and information continues to flow out of federal systems and private companies, and critical infrastructure remains susceptible (Coldabella & White, 2010).

A core DHS mission is to secure the key resources and critical infrastructure of the United States, including information technology and telecommunications systems, (Nojeim, 2010). To accomplish this DHS created the United Stated Computer Emergency Readiness Team (U.S. CERT) to provide 24-hour early watch warning and detection for the federal government's Internet infrastructure, and the leading program in this effort, EINSTEIN, was developed by U.S. CERT in partnership with the National Security Agency (NSA) and private industry (Chertoff, 2008)

Launched in 2004, EINSTEIN was meant to build and enhance national cyber-related situational awareness, identify and respond to cyber threats and attacks, improve network security, increase the resiliency of critical, electronically delivered government services, and enhance the survivability of the Internet. EINSTEIN was also developed to satisfy security mandates created by the Homeland Security Act and the Homeland Security Presidential Directive 7, and was intended to satisfy the Congressional requirements for information security outlined in the Federal Information Security Management Act (U.S. Department of Homeland Security, 2004).

EINSTEIN monitors network traffic and searches for signatures of known malicious code. When a pre-defined signature is identified, EINSTEIN alerts to the possibility of a network intrusion. The signatures themselves do not contain privacy sensitive information, or Personally Identifiable Information (PII) as defined by the DHS (Department of Homeland Security, 2004). However, the alerts that the second generation program (EINSTEIN II), and third generation program (EINSTEIN III) generates for U.S. CERT may include PII as they have the ability to read the content of message traffic, not just addressing information (Nojeim, 2010). Additionally, both the first and second versions of EINSTEIN monitored recorded copies of Internet traffic only, and only on the networks of participant government agencies. This meant that once malicious code was detected, the alert sent was merely a warning that an attack had already taken place (Nojeim, 2010).

EINSTEIN III however, monitors live traffic on the network in real-time, and also has the ability to counter the intrusion as it takes place (U.S. Department of Homeland Security, 2010). Like the previous versions of EINSTEIN, EINSTEIN III relies on pre-defined signatures of malicious code, but what is concerning is the combination of U.S. CERT's plans to deploy EINSTEIN III inside the networks of private telecommunications companies, and its ability to capture not only the data of the message exchange event, but also the content of the connection as well (Nojeim, 2010). The *EINSTEIN III Testing Exercise Privacy Impact Assessment* (PIA) gives as an example of this situation, an email in which the malicious code is contained in an attachment. In this situation, the PIA states that only the attachment, and not the content of the email, requires analysis. It does go on to say however, that, *sometimes the malicious payload is hidden and delivered via the content (or body) of the email*, and that in those cases, the analysis focuses only on the malicious payload, not on content, or PII contained in the content (U.S. Department of Homeland Security, 2010).

1. Terrorist Surveillance Program (TSP)

Following the terrorist acts of September 11, 2001 the National Security Agency (NSA), working with private telecommunications companies, began eavesdropping on

communications between persons both in the United States and abroad when one of the communications participants was suspected of being an agent of Al Qaeda or another terrorist organization. The program, known as the Terrorist Surveillance Program (TSP), aroused a sizeable amount of public objection as it seemingly violated The Foreign Intelligence Surveillance Act (FISA), which requires a court order for such surveillance. Additionally, the TSP placed participating private sector companies in an extremely difficult position, exposing them to potential litigation (Nojeim, 2010). The public outcry over the suspected abuses of power during the TSP program has increased the scrutiny of programs like EINSTEIN, and makes careful examination of legal issues and privacy protection particularly important prior to their implementation.

B. PURPOSE

This thesis will offer an in-depth analysis of the existing DHS document, *Privacy Impact Assessments for the EINSTEIN III*. It will examine strategies to address privacy concerns with the implementation of future EINSTEIN initiatives. In addition, this thesis will recommend the drafting of a new EINSTEIN III privacy policy, as well as a new legal opinion document that will balance the trade-off between privacy rights and the objectives of securing cyberspace. This is necessary to move forward with the implementation of this important network security system.

C. METHODOLOGY AND SCOPE

By reviewing current privacy policy and past privacy case studies, in addition to careful analysis of federal court cases and statutes, this thesis will establish the fundamental and constitutional right to privacy. Through secondary research this thesis will identify elements and exemptions of current communications legislation that can be used in the development of cyberspace monitoring policy that establishes proper legal foundations for the implementation of the controversial technology.

D. RESEARCH QUESTIONS

1. What are the fundamental principles of U.S. citizen's right to privacy?
2. How can U.S.-CERT simultaneously guard against the abuse of privacy rights while also preventing network intrusion and exploitation though the collection, analysis, and dissemination of sensitive information?
3. What protections should be put in place to prevent false identification and/or the initiation of actions against innocent system?

E. BENEFIT OF THE STUDY

Directors of all executive government agencies conducting cybersecurity operations will find this thesis useful in drafting policies and procedures to address privacy concerns in cyberspace. Moreover, the thesis will contribute to the body of literature addressing cybersecurity and privacy trade-offs by providing a comparative analysis of current government policies and current cybersecurity industry best practices.

F. ORGANIZATION OF THE THESIS

Research will first identify the right to privacy by exploring United States constitutional and case law. Next, the privacy concerns of leading civil rights organizations will be identified. A literature review will be conducted to gain a better understanding of current privacy and civil rights knowledge, and finally, changes to current EINSTEIN policy documents will be recommended.

II. THE FUNDAMENTAL RIGHT TO PRIVACY

A. HISTORICAL PERSPECTIVE

1. Evolution of Privacy Laws

The right to privacy is a fundamental human right and evidence of society's attempts to protect it can be found in the statues, constitutions and court rulings of nearly every democratic nation (Solove, 2008). Privacy provides freedom from scrutiny, prejudice, pressure to conform, exploitation, and the judgment of others. It is a prerequisite for freedom, democracy, well-being, individualism and innovation (DeCew, 2008).

The culture of privacy in the United States, and the rules and laws meant to protect it, are as old as the country itself. Early colonial American laws that dealt with privacy included those that protected, literally, against eavesdropping, which meant, *to stand within the drip from the eaves of a house to listen secretly* (Seipp, 1978). Additionally colonial american post services, which were under Brittish contol, were protected from privacy invasion by the Post Office Act of 1710. The act outlawed all but official tampering, or opening, of sealed mail (Lane, 2009). Of course, this led to an increase of *official* tampering, which most colonists viewed as an abuse of power. Additionally colonists viewed the colonial postal system as a tax, and chose to corresond via other means, or use shorthand or nicknames in their correspondence (Seipp, 1978).

Our nation's forefathers sought protections from excessive government power, and invasions of privacy, so, with the exception of the intelligence gathering via *dead letters* during the years of the Revolutionary War, Continental Congress's provisional New American Post Office, established rules against the opening, detaining, delaying or destroying of letters (Seipp, 1978).

Despite the evidence of these early attempts to protect the privacy of American citizens, some have argued that the right to privacy is not truly protected by the U.S.

Constitution because the subject is not specifically addressed in the documents text. Supreme Court Justice Hugo Black, in his dissent to the court's decision in Katz v. the United States argued that it was not the court's place to, rewrite the (Fourth) Amendment in order to bring it into harmony with the times (Katz v. United States). He stated:

> There can be no doubt that the Framers were aware of this practice, and, if they had desired to outlaw or restrict the use of evidence obtained by eavesdropping, I believe that they would have used the appropriate language to do so in the Fourth Amendment. They certainly would not have left such a task to the ingenuity of language-stretching judges. (Katz v. United States)

There have been many precedent setting cases brought before the Supreme Court challenging the right to privacy since Katz, and all have upheld the decision that despite the changes in the technology that has surrounded the suspected invasions of privacy, a person is protected from unwanted eavesdropping. While the U.S. Constitution does not specifically outline the protection of privacy, it was the court's decision then, and is still its decision today, that the protection is forged into the Bill of Rights; specifically via the Third, Fourth, and Fifth Amendments. Perhaps most specifically, the Fourth Amendment directly opposes government searches when a person has a, *reasonable expectation of privacy* (Solove, 2008).

Analysis of federal court cases and statutes will establish the fundamental and constitutional right to privacy, and is necessary for the development of the proposed policies that the Department of Homeland Security should employ to bolster public confidence in their ability to moderate the trade-off between defending the nation's system of computer networks, and protecting Fourth Amendment rights. Listed below are some of the most significant cases regarding the right to privacy in the United Stated, and these are followed by the federal statues that were derived from them.

B. CONSTITUTIONAL LAW

1. First Amendment

The First Amendment to the U.S. Constitution is probably the most widely known amendment, but is unlikely to be recognized as protecting privacy (The Revolutionary War and Beyond, 2012). The First amendment's primary intent is to protect the freedom of speech. It states:

> Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances. (U.S. Const. amend. I.)

The Amendment protects privacy by protecting the ability of citizen's to freely express themselves. If, for instance, a person knows that their private communications are being monitored, they would not likely feel free to engage in surreptitious speech, communicate openly, participate in political activities, or formulate original ideas, beliefs, and values. The First Amendment protects citizens from activities that prevent their freedom of speech and by extension their right to privacy (Solove, 2010).

2. Third Amendment

The Third Amendment protects the privacy of the home by preventing the requirement of citizens to house soldiers. It states:

> No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law (U.S. Const. amend. III).

Like the First Amendment, the Third protects the autonomy of U.S. Citizens, and their ability to make decisions about their beliefs, thoughts and political associations in private. By preventing the requirement to house soldiers, the Third Amendment protects the privacy and autonomy of a person within their home by inhibiting possible surveillance by soldiers being housed there (Lane, 2009).

3. Fourth Amendment

The Fourth Amendment, of all the amendments, is the one that most directly confronts the protection of privacy, as it safeguards citizens from unlimited search and seizures (U.S. Const. amend. V). It states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place (U.S. Const. amend. IV).

The Fourth Amendment serves as the structure upon which our current regulatory system for government information gathering is founded (Solove, 2010). The framers of the Constitution, could not have known that this single sentence would become the regulatory basis for all governmental information gathering, nor could they have forseeen the technological developments that would challenge it. The Amendment left many areas open for interpretation as new technologies arrived to challenge its protections of privacy, and the U.S. Supreme Court has attempted through the years to fill these voids with contitutional law. Today, all government information gathering activity requires that those searches be *reasonable;* meaning that they require a warrant supported by probable cause (Solove, 2010). By preventing *unreasonable* searches and seizures, the Fourth Amendment, and the regulatory system based on contitutional law, protects citizens' privacy in their aural and electronic communications, as well as their *person, house, or papers.*

4. Fifth Amendment

The Fifth Amendment protects citizens from being compelled to testify self-incriminating information, and guarantees the right to privacy with the *Due Process* clause. It says that a person:

> Shall [not] be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation. (U.S. Const. amend. V)

Like the Fourth Amendment, the Fifth Amendment seeks to protect privacy by extending the prevention of unreasonable searches and seizures of a person's records that might be held by a third party. Its relevance in government surveillance is important to note when third party private telecommunications companies are compelled to release information pertaining to their subscribers. Additionally the *Due Process* clause, of the Amendment, prevents governmental abuse of power that might threaten a person's liberty. This is accomplished through restrictions on the procedures the government can use in actions that might interfere with a person's liberty. By providing nation-wide protection, the doctrine recognizes that no procedure can be just if it is being used to unjustly deprive a person of their fundamental human rights (Dondershine, 2012).

5. Ninth Amendment

The Ninth Amendment can be viewed as being the universal amendment (Caplan, 1983). Specifically it states that, the enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people (U.S. Const. amend. IX.). Though the true meaning of the Ninth Amendment is vague, it has been interpreted in constitutional law as meaning a recognition that the Constitution is not an exhaustive listing of human rights, that additional fundamental rights, protected from governmental infringement, exist alongside those fundamental rights specifically mentioned in the first eight constitutional amendments, and that no part of the constitution should be construed to infringe upon these implicit rights (Caplan, 1983). Because the concept of privacy is not specifically addressed directly in either the Constitution or the Bill of Rights, the Ninth Amendment is often used as the basis for extending the application of other Amendments to the existance and protection of the fundamental right to privacy.

6. Fourteenth Amendment

The Fourteenth Amendments extends the Fifth Amendments Due Process clause to state law and constitutes another key piece to the doctrinal framework from which the right of privacy can be found (Schneider, 1988). The specific text, found in section one of the Amendment states:

> No state shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any state deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws (U.S. Const. amend. XIV.).

The Fourteenth Amendment prevents state's from drafting legislation that countermand protections of privacy provided for by the Constitution and the Bill of Rights, and it has been used by the Supreme Court to uphold protections for basic family privacy rights such as marriage, family relationships, family planning, and child rearing (Foxman & Kilcoyne, 1993).

C. CASE LAW

1. Definition

The legal system in the United States is based on the principle of *precedence*; a judicial doctrine that also serves as the analytical tool by which the rules of how to resolve legal disputes brought before the courts is guided (Kozel, 2010). Precedence means that the prior opinion of a court establishes the legal authority for future decision in court cases about the same legal questions; that if a court has already ruled on a given legal issue and another case arises with the same legal issue, the holding in the previous case will be applied to the new case (Hill & Hill, 2012). The practice of lower courts following a precedent is called *stare decisis*, which is Latin meaning, *to stand by a decision* (Hill & Hill, 2012).

Precedence and *stare decises* establish what is known as Case Law, which is distinguished from Statutory Law, the statutes and codes enacted by legislative bodies,

Regulatory Laws, which are regulations required by agencies based on statutes, and Common Law, which is generally accepted law (Administrative Office of the U.S. Courts, 2012). The following precedent setting cases serve as evidence of the Supreme Courts opinion that a person is protected from unwanted eavesdropping, and that every U.S. Citizen has a fundamental right to privacy.

2. Ex Parte Jackson

Protecting the privacy of citizens' communications is not a new concept. As early as 1782, laws were passed to prevent letter mail from being opened by unauthorized persons (Solove, 2006). Later in 1877, communications privacy was addressed by the Supreme Court in the case ***Ex parte Jackson***. Here the Court held that the Fourth Amendment prohibited government officials from opening letters without a warrant. They found that the amendment's guarantee that a person be secure in their papers against unreasonable searches and seizures was a guarantee not dependent on those papers being located inside the confines of a person's house; that the guarantee extends to their papers wherever they may be (Solove, 2006).

As with many laws, constitutional laws protecting privacy are not the application of abstract principles to specific facts, but are codified rules that are born of socially held beliefs and customs of proper behavior. Here the constitutional principle of communications privacy was the affirmation of long-standing law and custom, represented in the practices of the post office (Desai, 2007). The Fourth Amendment did not, on its own, give us the notion of communications privacy, but that that notion was a common held notion among the people; Ex parte Jackson effectively constitutionalized this notion. Today, we recognize that regardless of the technology used in our communications; be it a telephone conversation, emails, text or tweet; we expect that the constitutional principle of communications privacy be applied to it. Ex parte Jackson remains important today because it maintains this established principle (Desai, 2007).

Since Ex parte Jackson, many cases have shaped the laws surrounding the principle of communications privacy. In a 1960 survey of over 300 of these cases, renowned tort scholar William Prosser concluded that the cases recognized four distinct torts (Prosser, 1960):

(1) intrusion upon seclusion
(2) public disclosure of private facts
(3) false light or publicity
(4) appropriation

Of these, the tort of *intrusion upon seclusion* seems most relevant to communications privacy, as approached in the case of the EINTSTEIN III Intrusion Detection System (IDS), because protections from intrusions upon seclusion are meant to protect against electronic eavesdropping into conversations in the home (Solove, 2006). As defined by the *Restatement of Torts*, intrusion upon seclusion is committed by:

> One, who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person (Harvard University, 2012).

Although it is unclear whether evidence obtained via EINSTEIN can be used in a trial, the technology does still seem to intrude upon the seclusion of the victim, and the intrusion itself makes the defendant subject to liability, even though there is no publication or other use of any kind of the information outlined (Harvard University, 2012).

3. Olmstead v. United States

In 1928, in ***Olmstead v. United States***, the U.S. Supreme Court addressed whether wiretapping would be covered by the Fourth Amendment or left unregulated (Solove, 2006). The case involved Roy Olmstead a suspected bootlegger who was convicted in the Western District of Washington of a conspiracy to violate the National Prohibition Act by unlawfully possessing, transporting, importing and selling intoxicating liquors. His arrest, and subsequent conviction, was based on evidence gained through wiretaps in the

basement of his building and in the streets near his home that were placed without judicial approval. Olmstead argued that the wiretaps were a violation of his Fourth Amendment rights, and therefore the evidence gained by them should be thrown out (Olmstead v. United States).The Supreme Court however, upheld the conviction, concluding that the Fourth Amendment did not cover wiretapping because there was no entry of the houses or offices of the defendants (Solove, 2006).

Justice Louis Brandeis dissented to the Court's decision, arguing that new technological developments necessitated revising traditional views of the Fourth Amendment in order to preserve its purpose of protecting privacy (Solove, 2006). He believed that the Court's threshold test for determining Fourth Amendment coverage was narrow-minded and antiquated, and that the Fourth Amendment should be able to be adapted to apply to whatever technological means is being used to threaten the protection of privacy (Olmstead v. United States). He stated:

> Subtler and more far-reaching means of invading privacy have become available to the government. Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet (Olmstead v. United States).

4. Katz v. United States

In 1967, almost forty years after Olmstead, the Court finally embraced Justice Brandeis's opinion when it overruled the Olmstead decision in the case ***Katz v. United States*****.** In this case Federal agents attached an eavesdropping device to the outside of a public phone booth used by Katz on suspicion that he was transmitting gambling information over the phone to clients in other states. Based on the evidence obtained, Katz was convicted for the illegal transmission of wagering information. On appeal, Katz challenged his conviction arguing that the recordings could not be used as evidence against him based on his Fourth Amendment rights. The Court of Appeals however, rejected this point, noting the absence of a physical intrusion into the phone booth itself (Katz v. United States). This decision gave birth to the Court's current approach to determining whether the Fourth Amendment applies, *the reasonable expectation of*

privacy test. According to the Court, the overriding function of the Fourth Amendment is to protect personal privacy and dignity against unwarranted intrusion by the State (Solove, 2010). The reasonable expectation of privacy test articulated in Justice Harlan's concurrence, asks whether:

> (1) a person exhibits an actual or subjective expectation of privacy and
> (2) the expectation [is] one that society is prepared to recognize as *reasonable* (Solove, 2006)

The reasonable expectation of privacy test transforms the Amendment from outdated formalistic considerations, and re-focuses it on the basic principles of a right to privacy, no matter the domain of the trespass. The reasonable expectation of privacy test creates in the Fourth Amendment, the flexibility to evolve with society and remain connected to current social values (Solove, 2010).

5. Couch v. United States

In the 1973 case, ***Couch v. United States***, the petitioner (Couch) challenged that an Internal Revenue Service (IRS) summons directing her accountant to produce her (Couch's) business records. Couch claimed that the summons violated her Fifth Amendment right to prevent self-incrimination because the business records belonged to her, not her accountant. The District Court and the Court of Appeals concluded that the privilege against self-incrimination asserted by the petitioner was not available because she had effectively surrendered possession of the records to the accountant, and that there was no personal compulsion against her to produce the records personally. The Court found that the Fifth Amendment therefore constituted no bar to the production of the records by the accountant. Nor did the petitioner (Couch) have any legitimate expectation of privacy that would bar the production of the records (Couch v. United States). The Court determined that personal records maintained by third parties were not protected by the Fifth Amendment (Solove, 2006).

6. Smith v. Maryland

In the 1979 case, ***Smith v. Maryland,*** the victim (McDonough) was robbed, and after cooperating with the police, began receiving threatening phone calls from the robber (Smith). The telephone company, at police request, installed at its central offices a pen register to record the numbers dialed from the telephone at the petitioner's (Smith) home. Prior to his trial, Smith moved to suppress *all fruits derived from* the pen register on the grounds that it violated his Fourth Amendment rights. The Maryland trial court denied this motion, holding that the warrantless installation of the pen register did not violate the Fourth Amendment because it could not be applied to a list of the telephone numbers a person dials, as people, know that they must convey numerical information to the phone company and that the phone company records this information for billing purposes, therefore people cannot, harbor any general expectation that the numbers they dial will remain secret (Solove, 2006). On this basis Smith was convicted, and the Maryland Court of Appeals affirmed (Smith v. Maryland).

7. Doe v. Ashcroft/Gonzales/Mukasey/Holder

In 2004, the American Civil Liberties Union (ACLU) filed a lawsuit on behalf of a *John Doe* Internet Service Provider who had been served with a Federal Bureau of Investigations (FBI) National Security Letter (NSL). The lawsuit challenged whether the FBI had the authority to demand records and whether they could demand that NSL recipients be gagged from discussing record demands (American Civil Liberties Union, 2009).

In September 2004, the district court granted the plaintiffs' injunction but ordered a brief stay to allow the Government to appeal. The Second Circuit extended the stay, and Justice Ruth Bader Ginsburg, sitting as Circuit Justice, affirmed the extension (Nieland, 2007) (Jansen, 2006).

In March 2006, **w**ith the government appeal of the district court's September 2004 decision pending, Congress amended the Patriot Act to permit NSL recipients to consult a lawyer and seek judicial review of the letter's validity (Nieland, 2007). The amended Act

also modified the secrecy requirement permitting the FBI to continue to gag NSL recipients indefinitely. However, under the amended Patriot Act, the FBI would have to certify that the requirements for secrecy exist and recertify annually if the recipient challenges the necessity (Nieland, 2007).

In May 2006, the appeals court sent the case back to the district court to consider the constitutionality of the amended gag provisions, and in September 2007, the district court struck down the entirety of the NSL provisions of the Amended Patriot Act, ruling that the NSL statute's gag provisions violate the First Amendment right to free speech (American Civil Liberties Union, 2009) (Doe v. Gonzales, 2007).

In August 2009, after reviewing secret documents submitted by the government in an attempt to justify the continuation of the gag on Doe, the court ordered the government to partially disclose its secret filing and to release a public summary of its evidence (Doe v. Holder, 2009). Two months later, the district court ruled that the government could continue to enforce the five-year-old gag order on Doe and that the FBI could continue to suppress an *attachment* to the NSL Doe received (Doe v. Holder, 2009). Following this the ACLU filed a motion for reconsideration, and in March 2010, the Court ordered the government to release a less-redacted version of the attachment to the NSL issued to John Doe, but ruled that the government could continue to suppress certain information about the types of records the FBI demanded (Doe v. Holder, 2010). Five months later, in August 2010, the case was settled and the FBI lifted the gag on John Doe, who was then identified as Nick Merrill, president of New York-based Calyx Internet Access (Zetter, 2010).

D. FEDERAL ACTS

1. Definition

Federal Acts are Statutory Law, and are statutes and codes enacted by legislative bodies (Administrative Office of the U.S. Courts, 2012). In the United States, Statutory law are passed by Congress and approved by the President. Federal Acts are either: Public Law, relating to the general public, or Private Law, relating to specific institutions

or individuals (Brown & Williams, 2012). Most laws passed by Congress however, are public laws and these are the laws that apply to the right to privacy. The following sections examine key Federal Acts that form the legal protections meant to preserve the right to privacy.

2. Federal Communications Act

In 1934, six years after *Olmstead*, Congress enacted the Federal Communications Act (Solove, 2006). The Act combined and organized federal regulations covering telephone, telegraph, and radio communications, and created the Federal Communications Commission (FCC) to oversee and regulate these industries. As new communications technologies have been created, such as broadcast, cable, and satellite television, new provisions governing these communications have been added to the Act (47 U.S.C. 151, 1934)Of particular interest to the principle of communications privacy are the acts requirements that common carriers establish procedures to allow *appropriate authorization to activate interception of communications or access to call-identifying information* and *to maintain secure and accurate records of any interception or access with or without such authorization* (47 U.S.C. 151, 1934).

Section 605 of the Federal Communications Act provides for Fourth Amendment protection as it states:

> No person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communications to any person (47 U.S.C. 151, 1934).

However, the statute only applied to federal, not state, officials. According to the Supreme Court, section 605 prohibited evidence obtained by wiretapping from being used in court, but the statute did not restrict officials from engaging in wiretapping, only from disclosing intercepted communications in court proceedings (Solove, 2006).

Additionally, Section 606 provides for suspension or amendment of these rules and regulations by the president upon proclamation that *there exists a war or a threat of a war or state of public peril or disaster or other national emergency if he deems it*

necessary in the interests of national security or defense (47 U.S.C. 151, 1934). The president may prioritize defense or security communications, authorize government use or control of communications facilities, and suspend or amend rules and regulations applicable to any or all stations or devices capable of emitting electromagnetic radiations (47 U.S.C. 151, 1934).

3. Freedom of Information Act (1966)

In 1966 The Freedom of Information Act (FOIA) was enacted to amend the *Public Information* section of the Administrative Procedure Act (APA). The APA, in a reflection of governmental thought on records collection at the time, primarily provided for the withholding of government information, not its disclosure. The FOIA reversed this, and ushered in an era of full government disclosure, provided that the information being sought was not exempted under clearly delineated statutory language (Duke Law Journal, 1973). Specifically the Act states, that, *each agency, upon request for records which reasonably describes such records and is made in accordance with published rules stating the time, place, fees (if any), and procedures to be followed, shall make the records promptly available to any person.* (5 U.S.C. 552, 1966).

There are however, several exemptions to the disclosure requirements of the FOIA. The exemptions cover, among other things, national defense secrets, trade secrets, certain investigatory records compiled for law enforcement purposes, and certain inter- and intra-agency memoranda (5 U.S.C. 552, 1966). Of the Act's nine original exemptions, the sixth and seventh specifically seek to protect individual privacy. The sixth exemption states that the act's disclosure requirements do not apply to, *personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy,* and the seventh exemption excludes the requirement to disclose, *records or information compiled for law enforcement purposes…which could reasonably be expected to constitute an unwarranted invasion of personal privacy* (Solove, 2004). The scope and meaning of these exemptions was the

subject of considerable litigation and scholarly commentary, and ultimately led to the enactment of the Privacy Act of 1974, which is widely viewed as an amendment to FOIA (Duke Law Journal, 1973).

4. Title III of the Omnibus Crime Control and Safe Streets Act (1968)

In the years following the Supreme Court's Decision in *Katz*, Congress expanded protections against electronic surveillance beyond the limited protections of the Federal Communications Act with the introduction of Title III of the Omnibus Crime Control and Safe Streets Act. Title III extended the reach of wiretap regulations to state officials as well as to private parties. Despite these expanded protections it still only applied to the interception of aural communications; not to visual surveillance or other forms of electronic communication (Solove, 2006).

However, in its presently amended form, Title III does cover more than aural communications. Specifically it: (42 U.S.C. 3789D, 1968)

- prohibits the unauthorized, nonconsensual interception of wire, oral, or electronic communications by government agencies as well as private parties,
- establishes procedures for obtaining warrants to authorize wiretapping by government officials, and
- regulates the disclosure and use of authorized intercepted communications by investigative and law enforcement officers

There are some exceptions to the Act's protections however. The Act provides exceptions for operators and service providers for uses *in the normal course of (their) employment while engaged in any activity which is a necessary incident to the rendition of (their) service* and for *persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978* (42 U.S.C. 3789D, 1968). Additionally there is an exception to the requirement that government officials obtain a warrant before intercepting covered communications where:

> Any investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, or by the principal prosecuting attorney of any State or

> subdivision thereof acting pursuant to a statute of that state reasonably determines that an emergency situation exists that involves (42 U.S.C. 3789D, 1968).
>
> 1. immediate danger of death or serious physical injury to any person,
> 2. conspiratorial activities threatening the national security interest, or
> 3. conspiratorial activities characteristic of organized crime

5. Privacy Act of 1974

In 1973 the Department of Health Education and Welfare (HEW) issued a report titled, *Records, Computers, and the Rights of Citizens*, which analyzed the growing problem of personal information being collected and maintained by government agencies. The report recommended the passage of a code of *Fair Information Practices*, to prevent secret personal data record-keeping systems, provide individuals a means to find out what information about them is in a record and how it is used, and to allow an individual to prevent personal information from being obtained for one purpose and then be used or made available for other purposes without consent (Solove, 2006).

A year after the HEW report's recommendations, Congress passed the Privacy Act of 1974. The Act responded to many of the concerns raised by the HEW report, including regulation of the collection and use of records by federal agencies, and it established the right of individuals to access and correct personal information. The Act states that: (Solove, 2006).

> No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains.

The Act does however, have some shortcomings, first of which is that it does not apply to the private sector, state or local agencies. The Act also provides exceptions to the non-disclosure specification which include, but are not limited to, the permissible disclosure of records to, *agency employees maintaining records in the performance of their duties, the Census Bureau, persons using records for statistical reasons, national archiving, and to both houses of Congress* (5 U.S.C. 552a, 1974).

The most contentious of the act's shortcomings however, is the *routine use* exception, where information may be disclosed for any routine use if disclosure is compatible with the purpose for which the agency collected the information (Solove, 2006). The routine use exception states that:

> A record may be disclosed, for a routine use, where the term *routine use* means; with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected. (5 U.S.C. § 552a, 1974)

By definition, the use does not have to be for a purpose identical to the purpose for which the record was collected, only a *compatible* purpose, and this phrasing has led to uses of system of records in which the original routine uses for a particular database gradually increases until its scope is far beyond their originally stated goals (Electronic Privacy Information Center, 2012). In this way, the routine use exemption of the 1974 Privacy Act has been widely employed by agencies to allow disclosure of records without written consent of individuals (Straub & Collins, 1990).

6. Federal Intelligence Surveillance Act, FISA (1978)

In 1978 Congress enacted the Federal Intelligence Surveillance Act, FISA. FISA differs from Title III regulations in that it does not apply to electronic surveillance for domestic law enforcement purposes as Title III does; FISA is applicable when the purpose of the surveillance is to gather foreign intelligence. FISA permits electronic surveillance and covert searches pursuant to court orders issued after a review by a special court of seven federal judges, the Federal Intelligence Surveillance Court (FISC). Under FISA, orders are granted if there is probable cause to believe that the monitored party is a *foreign power* or *an agent of a foreign power*, and there is a showing of probable cause that the surveillance will uncover evidence of criminal activity (Solove, 2006). FISA protections are not as strong as the protections under Title III, and evidence obtained via surveillance permitted by FISC orders can be used in criminal trials.

7. Cable Communications Policy Act (CCPA)

In 1984 congress passed the Cable Communications Policy Act (CCPA) to protect the privacy of cable records. The Act protects the personal information of cable service provider customers, states that a cable company must notify subscribers about the collection and use of personal information, and that cable companies cannot disclose a subscriber's viewing habits (University of Miami, 2012) (Solove, 2006).

The CCPA does have a rather large exception, in that consent is not required to obtain information *necessary to render cable services*, nor is it required for information used to detect unauthorized reception (University of Miami, 2012). The CCPA specifically includes such other services as radio and wire communications, so it presumably applies to the personal use information of cable broadband Internet customer. However, the provisions of the CCPA probably will not apply to Direct Broadcast Satellite (DBS) companies that provide similar Internet services (University of Miami, 2012).

8. Electronic Communications Privacy Act, ECPA

The older Wiretap Act, Title III of the Omnibus Crime Control and Safe Streets Act of 1968, was originally written to address the interception of communications made via telephone lines. However, technological advances of many years mandated an update (Solove, 2006). As a result, Congress updated wiretapping law by modifying Title III. The resulting act, the Electronic Communications Privacy Act (ECPA) of 1986, expanded Title III to focus on new forms of communications, specifically those involving computers (Solove, 2006). The ECPA, as presently amended, protects wire, oral, and electronic communications while those communications are being made, are in transit, or when they are being stored on computers. The Act applies to email, telephone conversations, and data stored electronically (U.S. Department of Justice, Office of Justice Programs, 2012). The ECPA has three titles: Title I, known as the New Wiretap Act, regulates the interception of communications. Title II, referred to as the Stored Communications Act, protects the privacy of the contents of files stored by service providers and of records held about their subscribers, such as subscribers names, billing

records, or IP addresses. Title III addresses the requirement of government entities to obtain a court order authorizing the installation and use of a pen register and/or trap and trace device (18 U.S.C. 2510–22, 1986).

Title I provides the same exceptions as did its predecessor, Title III of the Omnibus Crime Control and Safe Streets Act. Here too, operators and service providers were authorized to monitor their customers, for uses in *normal activity necessary to the rendition of service* and for *persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, FISA*. Additionally, Title I provides procedures for Federal, State, and other government officers to obtain judicial authorization for intercepting such communications, and regulates the use and disclosure of information obtained through authorized wiretapping. The exception also states that a judge may issue a warrant authorizing interception of communications for up to 30 days upon a showing of probable cause that the interception will reveal evidence that an individual is committing, has committed, or is about to commit a particular offense (18 U.S.C. 2510–22, 1986).

9. Computer Matching and Privacy Act

In 1988 Congress passed the Computer Matching and Privacy Act to address an exception issues with the *routine use* clause of the 1974 Privacy Act. The Privacy Act stated that, a government agency can disclose private information without a written request by, or the prior written consent of, the individual to whom the record pertains, if disclosure of the record would be for a *routine use,* which was defined as use for a purpose which is compatible with the purpose for which it was collected (5 U.S.C. 552a, 1974).

As a means of detecting fraud, the federal government used this exception as the legal bases for running computer comparisons of employee records with the records of people receiving benefits, a practice known as *computer matching* (Solove, 2006). The Computer Matching and Privacy Protection Act of 1988 amended the Privacy Act to include procedural requirements for computer-matching activities, provide matching

subjects the opportunity to receive notice and to refute adverse information before having a benefit denied or terminated, additionally it required that agencies engaged in matching activities establish Data Protection Boards to oversee those activities (54 FR 25818, 1988).

The Act states that each agency that proposes to establish or make a significant change in a system of records, or a matching program, must provide adequate advance notice of the establishment or modification to the Committee on Government Operations of the House of Representatives, the Committee on Governmental Affairs of the Senate, and the Office of Management and Budget (OMB) in order to permit an evaluation of the probable or potential effect of such proposal on the privacy or other rights of individual (54 FR 25818, 1988). In essence the law establishes procedures for computer matching activities, but does not prevent the practice (Solove, 2006).

10. USA PATRIOT Act

In reaction to the terrorist attacks of September 11, 2001, Congress passed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, or USA PATRIOT Act. The Act loosened restrictions on federal officials' ability and authority to track and intercept communications for law enforcement and foreign intelligence gathering purposes, provided the Department of the Treasury regulatory powers to counter financial institution corruptions, and sought to tighten U.S. borders against foreign terrorists. Additionally the Act creates new crimes, new penalties, and new procedural efficiencies for use against domestic and international terrorists (U.S. Library of Congress, 2002).

The USA PATRIOT Act expanded the definition of pen registers and trap-and-trace devices established in the *Electronic Communications Privacy Act (ECPA)* to apply to addressing information on emails and to IP addresses. The Act expanded the circumstances under which the FBI could issue a National Security Letter (NSL), created new justifications for delayed notice of search warrants, and broadened the spectrum under which communications service provider subscriber records could be obtained (Nieland, 2007)(Solove, 2006). The Act made legal, roving wiretaps under FISA,

updating the law to reflect new technologies and new threats by allowing law enforcement officials to obtain a search warrant anywhere a terrorist-related activity occurred, and allowed victims of computer hacking to request law enforcement assistance in monitoring the trespassers on their computers (Solove, 2006)(U.S. Department of Justice, 2012).

11. REAL ID Act of 2005

Continued reactions to the September 11, 2001 terrorist acts led to the passage of the REAL ID Act in 2005 (Culotta & Fredrickson, 2007). The Act requires all Federal agencies to accept, for any official purpose, only those driver's licenses or identification cards issued by a state whose credentials comply with technical standards issued by the Department of Homeland Security. These standard's dictate how the state's issue driver's licenses, and defines in some detail what information those licenses must contain (Froomkin, 2007). Restrictions to those not carrying a properly credentialed card include domestic air travel and access to service benefits such as Social Security (Froomkin, 2007).

Although the cards are not federally issued, some see them as the beginning stages of the government building a central database for the collection of private information (Froomkin, 2007). The Electronic Frontier Foundation (EFF) believes that information in the databases will be used in a widening range of surveillance activities by government and businesses to access private information more easily. The American Civil Liberties Union believes that the databases will provide a one-stop shop for identity thieves, and others believe that the Act's requirement that the cards contain *Machine Readable Technology*, such as Radio Frequency Identification (RFID) tags, would allow for routine tracking, monitoring and regulating of citizen's movements and activities, because the RFID tags can be scanned from a distance (McLaughlin, 2007)(Smith, 2007)(Govindaiah, 2006). Additionally, since the cards contain both an individual's picture and date of birth, they have the potential to become de facto forms of identification used for many non-governmental transactions as well, such as entering a

bar, purchasing cigarettes or alcohol, or writing a check. This is a serious privacy concern because it makes it possible for those *private* transactions to be recorded, and stored (Govindaiah, 2006).

Proponents of the Act's card requirements say that the Act is not a mandate; that no state has to comply, but that those states that do not comply, cannot expect that their licenses will be accepted for federal purposes (McLaughlin, 2007). Others advocate the the use of imprinted barcodes to satisfy the Act's *Machine Readable* requirments because barcode readers interpret widths and heights to decode the stored data; therefore, requiring the holder to voluntarily pass the barcode through a scanner before the information contained can be attained. The argument here is that the inability to scan barcodes from a distance provides a level of security that protects privacy interests (Govindaiah, 2006). Additionally, some have stated that if RFID technology is to be used, the devices should employ encryption protection to directly affect privacy of the data stored (Govindaiah, 2006).

12. Homeland Security Presidential Directive 12, (HSPD 12)

Similar to the REAL ID Act, HSPD 12 established a mandatory, Government-wide standard for secure and reliable forms of identification for Federal Government employees and contractors (Presidential Directive 12, 2004). The Directive calls for *Secure and reliable forms of identification* that *is issued based on sound criteria for verifying an individual employee's identity, is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation, can be rapidly authenticated electronically and is issued only by providers whose reliability has been established by an official accreditation process* (Presidential Directive 12, 2004). An underlying goal of HSPD 12 is to protect the Federal Government's Internet infrastructure and computer systems against viruses and their potential to provide unauthorized access (Dasgupta, Chatha, & Gupta, 2007).

In response to HSPD 12, the National Institute of Standards and Technology (NIST) developed Federal Information Processing Standard Publication (FIPS PUB) 201 on Personal Identity Verification (PIV) (Karger, 2006). FIPS PUB 201 defines two kinds

of Personal Identity Verification (PIV) cards: PIV-I and PIV-II. (Karger, 2006). The difference being that the PIV-II cards are to incorporate smart card chips similar to the RFID chips in use on cards issued under the REAL ID Act. Printed on each PIV card will be the cardholder's name, photograph, the cardholder's organization, a serial number, an expiration date, and a variety of other agency-specific information. Data on the smart card chip includes, personal identification number (PIN) known by the card holder, a Card Holder Unique Identifier (CHUID), PIV authentication data consisting of an asymmetric key pair and corresponding certificate, and two biometric fingerprints (Karger, 2006).

The card will contain both contact smart card and contactless smart card interfaces. The contactless interfaces, like RFID chips, communicate over radio communications and are powered by transmissions from the reader itself, and like the RFID chip requires that the cardholder only be near the reader to have the information read (Karger, 2006).

E. SUMMARY

There have been many precedent setting cases brought before the Court challenging the right to privacy, and they all have led to the ultimate conclusion that, despite changes in technology, a person's privacy should be protected by law. Although the U.S. Constitution does not specifically outline the protection of privacy, the statutes, acts and court decisions of the last 200 years provide protections where a citizen has a, *reasonable expectation of privacy* (Solove, 2008). These many decisions, though not perfect, serve as the framework upon which all new privacy law or policy should be built. In this way, privacy policy can be conceptualized, and prevented from being bogged down and befuddled by the manifold complexities surrounding the issue of privacy itself (Solove, 2008). DHS policy drafters must incorporate, more densely, this historical privacy framework in their policies. Doing so will strengthen public confidence in their ability to moderate the trade-off between defending the nation's system of computer networks, and protecting privacy rights.

If the DHS's *Privacy Impact Assessments for the Initiative three Exercise (EINSTEIN)* is to be improved, its drafters must also address specific privacy concerns head-on. New technologies such as the EINSTEIN III IDS will, no doubt, continue to bring about questions surrounding privacy, and while it is true that no amount of research, policy or legal precedent will ever be the final answer to the question of privacy, the past must be deeply ingrained in future solutions (Solove, 2008). Incorporating answers to as many specific privacy concerns as possible is essential for public acceptance of such invasive technologies, and is what has to be done in all future policy documents surrounding the EINSTEIN III, IDS. A few of the most critical of these specific concerns are presented in the next section.

III. PRIVACY CONCERNS

A. OVERVIEW

The original version of EINSTEIN, EINSTEIN I, was an automated process for collecting, correlating, analyzing, and sharing computer security information across the Federal civilian government to increase awareness, in near real-time, of the threats to its infrastructure. EINSTEIN I sought to address common security weaknesses and promote the cyber security of government systems by providing worm detection, the ability to detect anomalous network activity, configuration management and trend analysis. EINSTEIN I worked by monitoring the network traffic of individual Internet users who browse, read pages, download information or otherwise communicate with a Federal Government (.gov) website (Department of Homeland Security, 2004). The security and network information about these transactions was collected and analysis conducted to provide situational awareness for Federal agencies concerning the state of Internet traffic across the Federal Government (.gov) domain. The information to be collected was only to be that which would be needed for analysis, and not interfere with the communications to and from agencies (Department of Homeland Security, 2004). Additionally, EINSTEIN I only collected data that would enable anomaly detection and other information technology risks, not personally identifiable information. These data were later identified as *network flow records*, and included data such as: source and destination IP address; source and destination port; the IP protocol; and associated derived metrics such as timing information and traffic volumes (Department of Homeland Security, 2008). No packet payload was stored in the flow records (Department of Homeland Security, 2004).

The follow-on version of EINSTEIN, EINSTEIN II, relied on commercially available intrusion detection capabilities that used a set of pre-defined signatures based upon known malicious network traffic, not personally identifiable information (PII). Nor was the IDS programmed to specifically collect or locate PII. Although EINSTEIN II did not seek or obtain the content of electronic communications, it was acknowledged that

future signatures might be developed in response to threats that use what appears to be PII, that the purpose of those signatures would be developed to prevent malicious activity from reaching federal networks, not to collect or locate PII (Department of Homeland Security, 2008).

EINSTEIN III intends to use a modified version of EINSTEIN I and EINSTEIN II, as well as a DHS test deployment of technology developed by the National Security Agency (NSA) that includes intrusion prevention capabilities. Additionally, EINSTEIN III proposes to demonstrate the ability of an existing Internet Service Provider, which would be designated as a Trusted Internet Connection Access Provider (TICAP), to select and redirect Internet traffic from a single participating government agency through EINSTEIN III technology (Nakashima, 2009). By doing so, U.S. CERT would be able to apply intrusion detection and prevention measures and generate automated alerts about selected cyber threats. All traffic handled by the TICAP that would be associated with the supplied IP addresses for the participating agency would be redirected to EINSTEIN III technology, and in that traffic there will be information that could be considered PII (Department of Homeland Security, 2010).

Concerns surrounding the privacy implications of the EINSTEIN III program, and pending legislation that appears to lay the legal groundwork for it, are well documented. Of the many questions surrounding the project those about the involvement of the National Security Agency (NSA) are most prominent, as many have concerns about the clandestine organization being permitted to use its computing and analytical powers to monitor the content of private Internet communications (Goldsmith, 2008**).** Private individuals and civil rights organizations are specifically concerned with potential capture of communications that have been mistakenly directed to systems under the protections of EINSTEIN III, the potential misuse of personal information that may be captured, the effects of such monitoring on free speech, and the possibility of monitored traffic being used as evidence in a court of law (Center For Democracy & Technology, 2009).

Questions surrounding EINSTEIN III and pending legislation vary, but the theme that underpins most concerns is that the program's secrecy alone undermines the

effectiveness of cybersecurity efforts, especially where the government is cooperating with private sector companies (Center For Democracy & Technology, 2009). In attempts to lift the veil of secrecey, several privacy and civil rights advocates have challenged the legitimacy of recent cybersecurity regulations and policies (Shaw, 2010). Of these the most active organizations are the Electronic Privacy Information Center (EPIC), the Center for Democracy and Technology (CDT), and the American Civil Liberties Union (ACLU). The overwhelming majority of cases come from EPIC, despite the ACLU's long history in civil rights issues. This is likely due to EPIC's concentration on cyberspace, while the ACLU has a wider civil liberties mandate that covers a greater scope than just issues involving electronics (Shaw, 2010).

B. ELECTRONIC PRIVACY INFORMATION CENTER (EPIC)

1. Background

The Electronic Privacy Information Center (EPIC) is a non-partisan public interest research organization established in 1994. EPIC's mission is to focus public attention on emerging privacy and civil liberties issues, with specific regard to computer security, privacy, and identification. Since its inception, EPIC has participated in numerous public debates regarding the protection of privacy rights on the Internet and elsewhere (Planning for the Future of Cyber Attack Attribution, 2010). EPIC's primary weapon in the fight for cyber privacy rights has been there use of Freedom of Information Act requests, and litigation when those requests have gone unanswered. As previously reviewed, The Freedom of Information Act (FOIA) of 1966 was enacted to amend the *Public Information* section of the Administrative Procedure Act (APA), which primarily provided for the withholding of government information, not its disclosure (Duke Law Journal, 1973). The era of full government disclosure, provided by the FOIA, has been responsible for uncovering numerous cases of government fraud and abuse since its inception. (Rotenberg, McCall, & Stepanovich, 2012)

Several successful EPIC FOIA cases highlight its ability to successfully employ FOIA requests and litigation to force disclosure of agency records (Why Isn't The

Department Of Homeland Security Meeing The President's Standard On FOIA, 2011). In a statement read before the Senate Judiciary Committee in March 2012, EPIC stated that: (Rotenberg, McCall, & Stepanovich, 2012)

> It is important that the NSA provide to the public, at a minimum, the legal basis of its authority to conduct cybersecurity within the United States. As we have repeatedly stressed in our filings, we simply cannot accept a doctrine of *secret law* in the United States for such a critical government function.

In regard to EINSTEIN, EPIC seeks disclosure that it hopes will shed light on the NSA's role in network monitoring, inadvertent capture of innocent communications, the potential misuse of personal information, the impact on free speech, and the 4th Amendment implications surrounding EINSTEIN, other cybersecurity related programs, and pending legislation in support of those initiatives (Rotenberg, McCall, & Stepanovich, 2012). A few of EPIC's more prominent attempts at seeking disclosure via FOIA requests are investigated below.

2. EPIC–Freedom of Information Act Requests & Litigation

EPIC is engaged in active litigation under the Freedom of Information Act with the NSA and National Security Council regarding National Security Presidential Directive 54, and EINSTEIN III (Planning for the Future of Cyber Attack Attribution, 2010). Between January 2009 and March 2012, EPIC pursued seven Freedom of Information Act requests with the NSA concerning cybersecurity operations. In six of those cases, the NSA did not disclose documents requested, ignored deadlines or refused to comply with required procedures, leading to FOIA Litigation (Rotenberg, McCall, & Stepanovich, 2012).

a. National Security Presidential Directive 54, FOIA

On June 25, 2009, EPIC submitted a Freedom of Information Act request to the NSA requesting the National Security Presidential Directive 54 (NSPD 54). NSPD 54, formalized the Comprehensive National Cybersecurity Initiative (CNCI), a multiagency, multiyear plan that lays out twelve steps to securing the federal

government's cyber networks, authorizes DHS, together with Office of Management and Budget (OMB), to establish minimum operational standards for Federal Executive Branch civilian networks in support of U.S. CERT's directing the operation and defense of government connections to the Internet (U.S. Department of Homeland Security, 2010a). The CNCI consists of a number of mutually reinforcing initiatives with goals designed to help secure the United States in cyberspace; one of goals is to d*eploy an intrusion detection system of sensors across the Federal enterprise*, and this goal is to be met with EINSTEIN (National Security Council, 2012). As of March 2012, neither NSPD 54 nor the CNCI had been released in whole, and only a partially declassified version of the CNCI was released following a lawsuit that was filed by EPIC against the NSA for its mishandling of the FOIA request (Rotenberg, McCall, & Stepanovich, 2012).

b. EINSTEIN III FOIA

On March 11, 2012, EPIC requested from the Department of Homeland Security, the Privacy Impact Assessment for the pilot exercise of EINSTEIN III, as well as *all contracts with private vendors, legal opinion, security analysis, and risk assessments concerning the program* (U.S. Department of Homeland Security, 2012). The Privacy Impact Assessment for the Initiative Three Exercise was published a week later on March 18, 2010 (Department of Homeland Security, 2010).

c. Lieutenant General Alexander Testimony FOIA

On April 16, 2010, EPIC requested from the NSA the *classified supplement* of Lieutenant General Keith Alexander's testimony before the Senate Armed Service Committee. The testimony contained his answers to questions posed by the Committee pursuant to his nomination to the position of NSA Director, Chief of the Central Security Service and Commander of the United States Cyber Command (CYBERCOM). General Alexander's public testimony raised concerns about the growing influence of the military in civilian cybersecurity efforts. Much of his remarks regarding the deployment of methods for monitoring electronic communications were classified, and the NSA has refused to make this information available. (Rotenberg, McCall, & Stepanovich, 2012)

d. EPIC–Google FOIA

On February 4, 2010 EPIC submitted a FOIA request to the NSA following media coverage of a possible partnership between the NSA and Google brought about because of an alleged cyber-attack by Chinese hackers. The FOIA request sought: (EPIC vs. NSA, 2011)

> All records concerning an agreement or similar basis for collaboration, between the NSA and Google regarding cyber security, all records of communication between the NSA and Google concerning Gmail, and all records of communications regarding the NSA's role in Google's decision regarding the failure to routinely deploy encryption for cloud-based computing service, such as Google Docs.

NSA responded to EPIC's request on March 10, 2010 by invoking Exemption Three of the FOIA and Section Six of the National Security Agency Act to issue a *Glomar* response, in which the agency neither confirmed nor denied the existence of any responsive records. An agency may issue a *Glomar* response when to answer the FOIA inquiry would *cause harm cognizable under an applicable statutory exemption*. The agency must demonstrate that acknowledging the mere existence of responsive records would disclose exempt information (EPIC vs. NSA, 2011).

EPIC filed suit in the district court challenging NSA's *Glomar* response and in support of its motion for summary judgment, the NSA filed a declaration by Diane M. Janosek, NSA Deputy Associate Director for Policy and Records (the *Janosek Declaration*). The district court on July 8, 2011, held that NSA was entitled to summary judgment because the *Janosek Declaration* was *both logical and plausible and contain[ed] sufficient detail, pursuant to Section 6, to support NSA's claim that the protected information [sought by EPIC] pertains to NSA's organization, functions, or activities* (EPIC vs. NSA, 2011). The Declaration further explained that if NSA disclosed whether records of cooperation or communications between Google and NSA existed, the disclosure of that information alone might reveal whether NSA investigated the threat, believed that the threat was a concern to the security of U.S. Government information systems, or took any measures in response (EPIC vs. NSA, 2011).

On May 11, 2012, the U.S. Court of Appeals affirmed the district court's opinion (EPIC vs. NSA, 2012). Given this precedent, it is likely that future FOIA requests surrounding EINSTEIN and related cybersecurity programs may be denied under the *Glomar* rule.

3. Cybersecurity Legislative Proposals

Pending cybersecurity legislation, The SECURE IT Act of 2012, and the Cybersecurity Act of 2012 both seek to amend the Federal Information Security Management Act (FISMA) by adding an exemption for information shared with or provided to a cybersecurity center (Rotenberg, McCall, & Stepanovich, 2012). EPIC, and several other civil liberty organizations, believe that provisions allowing different federal agencies to share information with DHS raise privacy challenges that need to be addressed. It is their belief that the FISMA reform authorizes federal agencies to share sensitive personally identifiable information with the Department of Homeland Security, authorizes DHS to disclose that information for law enforcement purposes, and that they may be intended to facilitate operation of EINSTEIN (Center for Democracy & Technology, 2012a).

a. The SECURE IT Act of 2012

On March 1, 2012 Several Senators, led by Senator John McCain, introduced the, *Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act (SECURE IT).* The proposed legislation intends to protect and secure the nation against cybersecurity attacks by promoting collaboration and information-sharing, updating criminal laws to account for the growing cyber threat and enhance research programs to protect critical networks (U.S. Senate Commitee on Energy & Natural Resources, 2012).

EPIC is concerned that some of the SECURE IT Act's proposed provisions damage the Freedom of Information Act; that its additional exemption for *information shared with or provided to cybersecurity centers*, as well as the proposed exemption three provisions, that would specifically exempt from disclosure all *cyber threat information* shared with the government, are ill conceived because *cyber threat*

information is defined broadly, and could include a large amount of information unrelated to cybersecurity (Rotenberg, McCall, & Stepanovich, 2012). Additionally EPIC believes that because the new provisions would be mandatory, agencies would be prohibited from disclosing information that they intended to make public or routinely available. In this way, EPIC believes the amendment could deny the public information that could assist in countering cyber threats, which might result in diminished public safety and national defense (Rotenberg, McCall, & Stepanovich, 2012).

EPIC says that the Act's provision governing disclosure of information to law enforcement which state that a, cybersecurity exchange that is a Federal entity may disclose cybersecurity threat indicator (if) the information appears to relate to a crime that has been, is being, or is about to be committed would, essentially, allow the government to flag any activity which may indicate a potential crime, including activities that are not part of a network intrusion. This practice could potentially violate search and seizure rights protected by the 4th amendment (Mills, 2012). EPIC believes that the Act fails to provide meaningful transparency and accountability protections, and that the handover of U.S. cybersecurity operations to the National Security Agency coupled with new exemptions from the Freedom of Information Act drastically limits public oversight necessary to prevent abuse and protect public privacy (Jackson, 2012).

b. The Cybersecurity Act of 2012

On February 15, 2012, Several Senators, led by Senator Joseph Lieberman, introduced the Cybersecurity Act of 2012. The Act is meant to enhance the security and resiliency of the cyber and communications infrastructure of the United States, and to provide the government with a clear structure for dealing with cybersecurity, including the security of critical infrastructure owned by the private sector (Cybersecurity Act, 2012) (U.S. Senate Commitee on Homeland Security & Governmental Affairs, 2012).

Similar to their concerns with SECURE IT, EPIC finds fault with the Cybersecurity Act of 2012's proposed *Exemption Three* provisions to exempt from disclosure *any cybersecurity threat indicator disclosed by a non-federal entity to a*

cybersecurity exchange. EPIC has found that the Act's definition of *cybersecurity threat indication* is mostly the same as the *cyber threat information* described in the SECURE IT Act of 2012. Here too, EPIC advocates the definition of *cybersecurity threat indicator* be subjected to public scrutiny and oversight in order to prevent abuse of discretion (Rotenberg, McCall, & Stepanovich, 2012).

C. CENTER FOR DEMOCRACY AND TECHNOLOGY (CDT)

1. Background

The Center for Democracy and Technology (CDT) is a nonprofit public policy organization and the leading Internet freedom organization. CDT's mission is to *conceptualize and implement public policies that will keep the Internet open, innovative, and free,* by preserving the unique nature of the Internet, enhancing freedom of expression, protecting privacy, and limiting government surveillance. CDT has advocated for groundbreaking legislation, won landmark court cases, promoted industry standards and practices, successfully argued before the Supreme Court for protecting free speech online, and strengthened privacy protection (Center for Democracy & Technology, 2012).

2. EINSTEIN IDS

Regarding EINSTEIN, other related cybersecurity programs, and pending legislation in support of these initiatives, CDT strongly disagrees with proposals to allow intra and inter-government information sharing by expanding government power to seize privately held data (Nojeim, 2009). CDT does not believe that a governmental entity should be involved in monitoring private communications networks as part of a cybersecurity initiative, but that it should be the job of the private sector communications service providers themselves (Nojeim, 2009). CDT also advocates an incremental approach to information sharing, with the understanding that routine monitoring of and sharing with law enforcement and intelligence agencies, communications from civilians

to the government will chill the exercise of the First Amendment rights of free speech and petitioning the government (Nojeim, 2009).

CDT criticizes the lack of transparency surrounding the EINSTEIN program and believes that it undermines the public trust that is essential to the success of its effort (Nojeim, 2009). Specifically, CDT questions whether EINSTEIN III's IP addresses screening method can reliably focus on only those communications that are intended for the government while excluding private-to-private communications (Nojeim, 2010).

3. Cybersecurity Legislative Proposals–Overview

CDT believes that the proposed cybersecurity legislation; The Cybersecurity Act of 2012 and the SECURE IT Act of 2012 would trump existing privacy laws and that they would permit more private information to be shared than is necessary. That these laws would allow information to be shared with law enforcement without the need for a warrant, and provide for inadequate accountability measures to ensure that the information sharing rules are followed. CDT is particularly opposed to the information sharing provisions of both bills that allow information to flow to the NSA (Center for Democracy & Technology, 2012a).

a. The SECURE IT Act of 2012

CDT is critical of the information sharing language in the SECURE IT Act that expressly allows sharing with the NSA, and allows ISPs to monitor for, and share with the NSA, any, *information that would foster situational awareness of the United States security posture* (Center for Democracy & Technology, 2012a). Additionally, CDT finds fault with the SECURE IT Act's provisions which allow information that is initially disclosed for cybersecurity purposes to be used for law enforcement purposes as well as for *national security* purposes unrelated to cybersecurity (Center for Democracy & Technology, 2012a). CDT believes that this could disrupt existing cybersecurity initiatives in the private sector, and that it could be used by government agencies to push industry in a direction that would not be desirable from a civil liberties standpoint (Center for Democracy & Technology, 2012a).

b. The Cybersecurity Act of 2012

Similar to its stance on the SECURE IT Act's information sharing provisions, the CDT finds fault with the Cybersecurity Act allowing information initially disclosed for cybersecurity purposes to be used for other law enforcement purposes. Specifically, CDT believes that language in the bill which states, *information that appears to relate to a crime can be disclosed to law enforcement* creates a backdoor warrantless wiretap (Center for Democracy & Technology, 2012a).

CDT is critical of the Act's broad classifications of information systems as being considered critical infrastructure information systems, and warns that a policy that treats all critical infrastructure information systems the same threatens elements of the Internet and communications structure critical to new economic models, human development, free speech and privacy; potentially stifling innovation, chilling free speech and violating privacy rights. (Nojeim, 2009)

CDT is also critical of the Act's FISMA reform provisions which authorizes federal agencies to share sensitive personally identifiable information (PII) with the Department of Homeland Security and also authorizes DHS to disclose that information for law enforcement purposes. CDT believes that these provisions are specifically intended to facilitate the operation of EINSTEIN technology (Center for Democracy & Technology, 2012a).

D. AMERICAN CIVIL LIBERTIES UNION (ACLU)

Despite its long history with advocating privacy rights, the ACLU has little to say regarding the EINTEIN program. The ACLU Northern California Division, on its website simply states about EINSTEIN that: (American Civil Liberties Union, 2012)

> Having privacy impact assessments and policies are necessary but not sufficient to protect privacy. Nor are promises to not retain the data after the traffic analysis – there needs to be regular, consistent oversight and monitoring of the program – the kind of oversight that did not occur to prevent the abuse of National Security Letters by the FBI . Cyber-security is a very critical issue, but developing more ways to snoop on the online activities of innocent Americans, with no showing of suspicious or

> harmful activity is not the way to deal with it. As the Congressional leaders understood, this program should not go forward.

Similarly, the ACLU opposes a proposed amendment to the pending Cyber Intelligence Sharing and Protection Act (CISPA) that would permit surveillance systems that are even broader and stronger than EINSTEIN. The ACLU believes that the proposed amendment is broad enough to include government contractors and university networks, and authorizes Homeland Security to intercept a large portion of Web and email communications and *deploy countermeasures* against Internet-based adversaries (McCullagh, 2012). Opposition from the ACLU stems from the section of CISPA that says *notwithstanding any other provision of law,* companies may share information with the government. The ACLU believes that the word *notwithstanding*, seems to make the legislation trump all existing federal and state civil and criminal laws, and that that makes it a clear threat to First Amendment freedom of speech rights as well as Fourth Amendment privacy rights (McCullagh, 2012).

E. CONGRESSIONAL RESEARCH GROUP (CRS)

Civil rights organizations are not alone with their concerns about EINSTEIN. Many members of Congress have also been critical of the program. On April 2012, the Congressional Research Service (CRS) published a report for members and committees of Congress outlining those concerns. Specifically the research group found that EINSTEIN's monitoring of all communications coming to and from federal agency computers posed significant privacy implications, and would most likely violate Fourth Amendment guarantees of being free from unreasonable searches and excessive government intrusion (U.S. Library of Congress, 2012). CRS acknowledged DHS's development of procedures to address privacy concerns; including the minimization of information collection, training, accountability requirements, and retention rules, but does not believe that they go far enough to preserve privacy interests protected under the Fourth Amendment. (U.S. Library of Congress, 2012)

1. The Expectation of Privacy

CRS does believe that, in some instances, monitoring of networks might not violate Fourth Amendment protections, and that for those protections to apply, a court must first inquire whether the monitoring constitutes a *search* or *seizure* in the constitutional sense (U.S. Library of Congress, 2012). This means that if a *search* has occurred, a court will have to determine first, whether the individual had an actual expectation of privacy that society would deem reasonable; and if so, the court could then ask if the search was reasonable. Typically a search would not be reasonable unless the government obtains a warrant based upon probable cause, but there are, exceptions to this rule such as special needs and consent (U.S. Library of Congress, 2012).

The CRS report cites the legal case *United States v. Warshak* as an example where a court upheld the principle of an individual having a legitimate expectation of privacy in the *content* of communications. In this case, the report says the Ninth Circuit ruled that a *subscriber enjoys a reasonable expectation of privacy in the contents of emails that are stored with, or sent or received through, a commercial Internet Service Provider (ISP)* (U.S. Library of Congress, 2012). Based on this the CRS believes that because EINSTEIN III not only collects the routing, non-content portions of communications, such as email header information, but also scans and collects the content of the communications, such as the body of emails, that individuals most likely have a reasonable expectation of privacy in those electronic communications. The CRS Report further outlines that the EINSTEIN program requires a Fourth Amendment inquiry into two discrete classes of individuals: (1) federal agency employees who access federal networks while at work; and (2) private persons who either contact a federal agency directly or who communicate via the Internet with a federal employee. CRS believes that the Fourth Amendment rights of the former primarily rest on cases dealing with privacy in the workplace and consent, while the latter requires a broader look at privacy and electronic communications (U.S. Library of Congress, 2012).

2. Federal Employees

Regarding the monitoring of federal agency employees, CRS says that answers to questions about the use of log-on banners, computer user agreements, and the scope of non-investigatory, work-related monitoring, are unclear. They cite the case *City of Ontario v. Quon*, where the Supreme Court upheld, under the Fourth Amendment, the city's search of text messages sent on a city-issued pager by a police officer employed by that city. The Court assumed that the employee had a reasonable expectation of privacy in sent text messages, and that the review of those text messages constituted a search. The Court's decision meant that the same rules that applied to a search of an employee's office also apply equally to an intrusion into his electronic communications. However, the Court then applied the *special needs exception* to the warrant requirement, which holds that a government employer need not get a warrant to conduct a search when the search is done for a *non-investigatory, work-related purpose* (U.S. Library of Congress, 2012).

Like the policy of the City of Ontario, a condition of enrolling in EINSTEIN requires participant federal agencies to certify that certain log-on banners or computer user agreements are in place to ensure employees are aware of and consent to the monitoring, interception, and search of their communications on federal systems.
Based on this, the Department of Justice's Office of Legal Counsel believes that the use of the log-on banners on all federal computers will eliminate any expectation of privacy in communications transmitted over those systems. CRS points out however, that, *Quon* was limited to searches for a *non-investigatory work-related purpose*, and that if EINSTEIN could be seen as overreaching this permissible purpose, by scanning emails for unlawful activity instead of malicious computer activity, a court may find its scope a violation of the Fourth Amendment (U.S. Library of Congress, 2012).

3. Private Citizens

CRS believes that privacy issues surrounding communications sent by a private person to a federal employee via governmental email or personal email account are more serious than those surrounding the communications of federal employees because the

private citizen has neither consented to monitoring by clicking on a log-on banner nor signed a user agreement. CRS recognizes that the third-party doctrine, which seeks to protect privacy by extending the prevention of unreasonable searches and seizures of a person's records held by a third party, could arguably permit EINSTEIN's monitoring of private citizens. However, CRS notes that court cases such as *Smith v. Maryland* and *United States v. Warshak* have significantly diminished protections provided by the third party doctrine, and that these third-party cases also traditionally applied only to non-content information (U.S. Library of Congress, 2012).

4. The Special Needs Exemption

CRS's stance is that, if the assumption is made that both federal employees and those communicating with them have a reasonable expectation of privacy in the contents of their communications, EINSTEIN has to then be tested under the general reasonableness requirement of the Fourth Amendment which requires that all government information gathering activities require that those searches be *reasonable;* meaning that they require a warrant supported by probable cause (Solove, 2010).

Here, the CRS report points out arguments in favor of applying the *special needs exception,* where Courts have held that *when there are special governmental needs, beyond normal law enforcement,* the government may need neither a warrant nor any level of individualized suspicion. The CRS report gives as examples of such cases, the rules used to support sobriety roadblocks and border searches. The report suggests that an argument could be made that the impracticality of obtaining a warrant for a cyber-threat, and that since the purpose of the EINSTEIN program is beyond normal law enforcement, the application of the special needs doctrine to the EINSTEIN program may be justified (U.S. Library of Congress, 2012).

F. SUMMARY

Although the concerns of private individuals, civil rights organizations and the U.S. Congress are clear. Specific concerns about the EINSTEIN programs capabilities are not well defined. Most significant opposition to the program seems to be centered on the

disclosure of exactly how the program operates, what information it has the potential to collect, to what extent the NSA will be involved, and how the potential capture of communications that have been mistakenly directed to systems under the protections of EINSTEIN might potentially be misused. Through FOIA requests EPIC seeks to gain insight into the unknown operations of EINSTEIN that might help to answer these questions, while CDT, the ACLU and CRS, focus on privacy implications based on what is known about EINSTEIN.

To quell the concerns of these organizations, DHS's *Privacy Impact Assessments for the Initiative three Exercise (EINSTEIN)* should reveal as much information regarding the technical operations of the program as security will allow, and where security will not, a classified version should be made available to Congressional Committees that have the requisite level of security clearance. This level of disclosure could satisfy EPIC's desire for greater insight into the unknown operations of EINSTEIN, and also give greater clarity about the legal implications to the other concerned organizations.

IV. LITERATURE REVIEW

A. DHS PRIVACY POLICY FOR EINSTEIN

1. EINSTEIN III Testing Exercise Privacy Impact Assessment (PIA)

The *EINSTEIN III Testing Exercise Privacy Impact Assessment (PIA)*, states that the exercise's purpose is to,

> Demonstrate the ability of an existing Internet Service Provider, that is designated as a Trusted Internet Connection Access Provider (TICAP) to select and redirect Internet traffic from a single participating government agency through the Exercise technology, for U.S. CERT to apply intrusion detection and prevention measures to that traffic and for U.S. CERT to generate automated alerts about selected cyber threats. (U.S. Department of Homeland Security, 2010)

The report goes on to state that the PIA is being conducted because the Internet traffic being analyzed might contain Personally Identifiable Information (PII), and that locations for deploying the technology somewhere other than private telecommunications companies networks were considered and ruled out due to cost, scalability, network coverage and speed of implementation (U.S. Department of Homeland Security, 2010).

To conduct the exercise, participating government agencies would supply a list of IP addresses to the Trusted Internet Connection Access Providers (TICAP), which will designate what Internet traffic is destined for, or coming from participating agency systems (U.S. Department of Homeland Security 2010). Once the TICAP has identified this, they will verify the traffic is in fact only the participating agency's traffic, and redirect the traffic to a secured facility where the EINSTEIN technology will analyze it (U.S. Department of Homeland Security, 2010). Additionally, the PIA states that only the limited portion of the redirected traffic that is associated with identified cyber threats will be available to U.S. CERT analysts for review, and that U.S. CERT will analyze this data, *in accordance with written information handling procedures* (U.S. Department of Homeland Security, 2010). Including procedures to, *identify information that could be*

considered PII, verify whether the information specifically links to an individual, and purge that information from the analysis unless it is necessary for further U.S. CERT analysis (U.S. Department of Homeland Security, 2010).

Written information handling procedures, as described in the EINSTEIN III Testing Exercise Privacy Impact Assessment (PIA), state that U.S. CERT personnel must determine that PII, if collected, is required for later analysis before it is further processed or retained, and that information deemed unnecessary for further analysis is to be purged. If and when PII is used, U.S. CERT's information handling procedures require that U.S. CERT personnel summarize and document why the information is necessary, including a description of the cyber threat, the information in question, and why further analysis of the information is necessary. Additionally, both the U.S. CERT Director and Deputy Director would be provided weekly summaries of all instances when PII was deemed necessary for further analysis, and that the process would be periodically reviewed by the Oversight and Compliance Offices of U.S. CERT and The Office of Cybersecurity and Communications (CS&C) (U.S. Department of Homeland Security, 2010).

The EINSTEIN III Testing Exercise Privacy Impact Assessment (PIA) also addresses the possibility of non-governmentally provided IP Addresses being mistakenly monitored, resulting in the PII of Internet traffic not destined to, or originating from government computer networks being collected. The PIA states that in this event the PII, *will be removed and U.S. CERT will analyze the situation and provide remedial actions* (U.S. Department of Homeland Security, 2010). False Positives, or misidentified malicious code and the subsequent alerting to Internet traffic and/or preventing transmission, are to be documented to include the nature of those false positives, including the specific information generated by the faulty signature (particularly if that data includes PII), and data of false positives is to be removed or modified to eliminate future false positive events (U.S. Department of Homeland Security, 2010).

The EINSTEIN III Testing Exercise Privacy Impact Assessment (PIA) rests on legal analysis provided during the Preceding EINSTEIN II Exercise (Bradbury, 2012). The legal opinions, as explained in the U.S. Department of Justice Office of Legal Counsel's reports: *Legality of Intrusion-Detection System to Protect Unclassified*

Computer Networks in the Executive Branch, and *Legal Issues relating to the Testing, Use, and Deployment of an Intrusion-Detection System (EINSTEIN 2.0) to Protect Unclassified Computer Networks in the Executive Branch*, both conclude that user consent is given to the monitoring of network traffic to and from government agency computer networks by implementing and enforcing the use of *model log-on banners* (Bradbury, 2012). The PIA states that:

> The decision to use the participating agency's network or communicate electronically with the agency is essentially the decision to provide network flow records and the other network traffic that will be scanned with the Exercise technology. (U.S. Department of Homeland Security, 2010)

Additionally the legal opinions state that government employees give consent to the search by agreeing to a *computer-users agreement* that notifies them of monitoring, and that any person sending information to a government employee is not privy to a reasonable right to privacy in regard to their communications, as they *cannot object if the third party conveys that information or records thereof to law enforcement authorities* (Bradbury, 2012).

B. PRIOR STUDIES

1. Striking the Right Balance, Tina M. Skahill

In her thesis, Tina M. Skahill examines fusion center policy, and recommends policy options to simultaneously safeguard against abuse of citizens' privacy while facilitating the collection, maintenance, and dissemination of information (Skahill, 2010). Principally, the analysis identified that fusion center's collection, analysis, and dissemination of information derived from the various participating sources, have a profound impact upon the Fourth Amendment right to privacy, and that this activity is the most controversial privacy issues regarding fusion centers (Skahill, 2010). The thesis also identified that individual agencies participating in fusion center activity mostly adhered

to states' privacy laws, and that this adherence encouraged policy shopping, meaning that agencies adhered to local policy, although it contradicted the policy of their agency, or vice versa (Skahill, 2010).

Also identified in the thesis was that guidelines issued by federal agencies such as DHS and DOJ, failed to address the reconciliation of community-policing principles with fusion center operations, and that the failure of adequately addressing the competing principles of security and transparency resulted in inconsistencies among fusion centers (Skahill, 2010). The thesis also identified that the guidelines recommending self-conducted privacy-impact assessments, fail to address the inherent problem with an agency conducting its own assessments (Skahill, 2010).

2. Cybersecurity and Freedom on the Internet, Gregory T. Nojiem

In this article the researchers' acknowledge the importance of cybersecurity programs and policy and also acknowledge the need to monitor traffic to and from government networks. However, the researchers' contend that protecting these systems cannot be accomplished if they threaten user privacy, or innovation. The researchers' argue that cybersecurity programs can only be successful if they encourage private industry participation instead of mandating it. The researchers' state that legal issues are covered, initially, by consent, and secondly by *self-defense* provisions of current laws that allow information sharing from private companies to government agencies. However, the article claims that privacy issues do not stop there, as the problem of inadvertent capture of private information is not addressed. Also that no measures are in place to prevent misuse of information by the private communications companies themselves and that the role of law enforcement and intelligence is not clear (Nojeim, 2010). Instead of requiring the participation of private companies, the researchers' advocate giving incentives to private companies to encourage their sharing of threat information (Nojeim, 2010).

In regard to the EINSTEIN Program, the article warns that if Einstein III were to analyze private-to-private communications, the interception would likely be considered an interception under the electronic surveillance laws, requiring a court order. To remedy

this, the article calls for an independent audit mechanism to ensure that such private-to-private communications are not scrutinized (Nojeim, 2010).

3. *Privacy*, Linda Koontz

In her testimony before the Senate's Committee on Homeland Security and Governmental Affairs, Linda Koontz, argues that although privacy laws and guidance set minimum requirements for agencies, in regard to the collection of PII, they fail to do so consistently throughout the federal government and that they may not fully adhere to key privacy principles (Koontz, 2008). She raises concerns that, *the framework of legal mechanisms for protecting personal privacy that has been developed over the years may no longer be sufficient, given current practices* (Koontz, 2008). The GAO's opinion, as testified by Mrs. Koontz, is that for the government to strike the correct balance between the need to collect and use information, while also preserving privacy rights, privacy protection application must be consistent across all federal activities, and limited use of personally identifiable information collected must be assured (Koontz, 2008).

Federal agencies' use of personal information is governed by the Privacy Act of 1974 and the E-Government Act of 2002, and in her testimony Mrs. Koontz claims that the Privacy Act's definition of *system of records*, which sets the scope of the acts protection, is too narrow in scope, and does not always apply to all information collected (Koontz, 2008). She explains that the Act's definition of a record as, *A group of records that is under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual* allows for several ways in which personally identifiable information might be collected outside the Act's definition, and therefore not be protected by it (5 U.S.C. 552a, 1974). She gives as example, data mining, where a system performs analysis by looking for patterns of personal information located in other systems of records or performs subject-based queries across multiple data sources that may not constitute systems of record under the act (Koontz, 2008). Mrs. Koontz suggests

that to address these issues, the system-of-records definition be revised to cover all personally identifiable information collected, used, and maintained systematically by the federal government (Koontz, 2008).

In discussing the issue of ensuring the limited use of personally identifiable information collected, Mrs. Koontz states that there are insufficient specificity requirements of purpose descriptions in public notices, and that inconsistency in the definition of routine uses across federal agencies weakens use limitations. She argues that the Privacy Act's limitations on the usage of PII within an agency are overly modest; that the Privacy Act may not apply to data shared between agencies, and that broad specification of purpose could lead to unreasonable ranges of use, calling into question the legitimacy of meaningful limitations (Koontz, 2008). She argues that the current practice of agencies limiting information internally, only to those with a need to know, does not take necessary steps to limit the use of this information (Koontz, 2008). Mrs. Koontz also states that while the Privacy Act provides protections for information that is in systems-of records, it does not protect data after they have been disclosed to other agencies, and that data shared outside could fall subject to misuse. To correct these deficiencies Mrs. Koontz suggest that laws or guidance be revised to require agencies to justify the use of key elements of personal information, set specific limits on routine uses and internal agency use of personal information, and that they also require agencies to establish formal agreements with external entities before sharing personal information with them (Koontz, 2008).

4. Square Legal Pegs in Round Cyber Holes, John N. Greer

This article argued that current laws governing intelligence agencies, such as the NSA, were established in a pre-cyberspace world, and that the NSA's dual roles of being an intelligence collection agency operating outside the United States, and a defender of national information systems domestically, thwarts the agencies efforts to maintain the trust of the American people (Greer, 2010). The researcher argued that the digital age and evolution of the cyberspace environment make it inappropriate to think of threats in terms of geographical boundaries, explores the need to interpret existing legal authority in the

new cyberspace world, and how to achieve the balance between securing the nations networks and protecting the privacy of U.S citizens (Greer, 2010).

The article calls for the creation of a central organization to gather information from multiple sources including federal, state, local, foreign and private sources, to generate a common operating picture of global network status. The article recognized that this arrangement would create a myriad of legal complications, and suggested tagging data elements collected with information such as authorities and restrictions, and that data collected by the center be limited to those with proper authority. The article also suggested that it might be necessary to draft regulations making the sharing of data mandatory for owners of critical infrastructure (Greer, 2010). The article called for an amendment of the minimization procedures governing the sharing of Signals Intelligence (SIGINT) information, as currently the Supreme Court has ruled that the interception of electronic communications falls under the purview of the Fourth Amendment; meaning the NSA can provide SIGINT to customer agencies within the federal government only after it is has been evaluated and reviewed for minimization procedures, a process that makes the sharing of threat information in real-time impossible (Greer, 2010).

The article supports NSA cybersecurity activities that are subject to oversight both internally and externally. Internally, the article listed: component oversight and compliance officers, component-level training, and reviews by the Offices of General Counsel and Inspector General, and an Agency Privacy and Civil Liberties officers. Externally it listed: review by the Department of Justice, the Intelligence Oversight Board, the Office of the Director of National Intelligence Civil Liberties Protection Officer, and the Privacy and Civil Liberties Oversight Board, the Armed Services, Intelligence, Judiciary, and Government Reform Committees of Congress, and the Judicial Branch, by reviewing applications to the FISC (Greer, 2010).

C. GAPS IN THE POLICY

1. Lack of Review of PII Weekly Summary by Outside Agency

The EINSTEIN III Testing Exercise Privacy Impact Assessment (PIA) stated that there is a requirement that U.S. CERT personnel determine if collected PII is required for later analysis before it is further processed or retained, and that information deemed unnecessary for further analysis be purged. The PIA also stated that when PII is used, information handling procedures require that U.S. CERT personnel summarize and document why the information is necessary, and that, both the U.S. CERT Director and Deputy Director be provided weekly summaries of all instances when PII was deemed necessary for further analysis; a process that is subject to periodic review by the Oversight and Compliance Offices of U.S. CERT and The Office of Cybersecurity and Communications (CS&C) (Department of Homeland Security, 2010). Not covered by the PIA is that no one outside the DHS has oversight into the procedure, and that without outside oversight a conflict of interest may allow the misuse of PII to go unchecked.

2. No Description of Remedial Action

The EINSTEIN III Exercise PIA addresses the possibility of non-governmentally provided IP addresses being mistakenly monitored, and Internet traffic not destined to, or originating from government computer networks being collected. In the event of this happening the PIA states that the traffic will be removed and U.S. CERT will analyze the situation and provide remedial actions. However, the PIA gives no further description of the remedial action that will be taken, nor does it describe any procedure to notify the originators of the misdirected traffic of inadvertent capture of their traffic without their consent. Further, the PIA does not provide redress instructions for the originators of the misdirected traffic.

3. Legal Opinions Based on EINSTEIN II Capabilities

The U.S. Department of Justice Office of Legal Counsel's opinions, *Legality of Intrusion-Detection System to Protect Unclassified Computer Networks in the Executive*

Branch, and *Legal Issues relating to the Testing, Use, and Deployment of an Intrusion-Detection System (EINSTEIN 2.0) to Protect Unclassified Computer Networks in the Executive Branch*, stands as the legal justification for conducting the EINSTEIN III Exercise (Bradbury, 2012). The opinion states that users consent to monitoring by clicking through model log-on banners (Bradbury, 2012). Additionally, the legal opinions state that government employees give consent to the search by agreeing to a computer-users agreement that notifies them of monitoring, and that any person sending information to a government employee is not privy to a reasonable right to privacy in regard to their communications, as they cannot object if the third party conveys that information or records thereof to law enforcement authorities (Bradbury, 2012).

However, these legal opinions were based on the capabilities of EINSTEIN II, which was deployed on the networks of participant government agencies only. EINSTEIN III monitors traffic on live networks of private telecommunication providers (Department of Homeland Security, 2010). The legal opinions do not take into account the issue of consent not being obtained by all of the customers of the participant private telecommunication providers. If PII is obtained through Internet traffic that was mistakenly monitored, the absence of consent by the private telecommunication provider's customer would, according to the legal opinions used in the EINSTEIN III PIA, be considered an illegal search based on the requirements of the Wiretap Act, FISA, SCA and the Pen/Trap Act (Bradbury, 2012).

D. GAPS IN THE LITERATURE

1. Fourth Amendment Rights Not Addressed

The thesis, *Striking the Right Balance: Fusion Centers and Privacy* (Skahill, 2010) provided valuable insight into the issue of Security vs. Privacy, particularly with regard to government policy, and policy documents. However, the thesis focused primarily on the practice of information sharing between federal and local government entities, and did not provide analysis of collecting or monitor PII in cyberspace.

Particularly the Fourth Amendment right to protection from warrantless search and seizure, and how it should be applied to searches in cyberspace are not addressed.

2. Literature Fails to Address the Lack of Remediation Procedures

The article *Cybersecurity and Freedom on the Internet* (Nojiem, 2010), states that the legal issues of monitoring Internet traffic are covered, initially, by consent, and secondly by self-defense provisions of current laws that allow information sharing from private companies to government agencies (Nojeim, 2010). The author did however, address the fact that inadvertent capture of private information was not addressed, and that no measures were in place to prevent misuse of information by the private communications companies (Nojeim, 2010). In regard to the EINSTEIN Program, the author said that if Einstein III were to analyze private-to-private communications, the interception would likely be considered an interception under the electronic surveillance laws, requiring a court order. To remedy this, the article called for an independent audit mechanism to ensure that such private-to-private communications are not scrutinized (Nojeim, 2010). The article however, does not address the lack of remediation procedures for the inadvertent capture of private information.

The article, *Privacy; Congress Should Consider Alternatives for Strengthening Protection of Personally Identifiable Information* (Koontz, 2008), approaches the issue of monitoring Internet traffic by addressing the scope of the Privacy Act's definition of system of records. Here the researcher argues that the Act's narrow definition allows for several ways in which personally identifiable information might be collected outside the Act's definition, skirting the protection it provides. The researcher suggests that to address this issue, the system-of-records definition be revised to cover all personally identifiable information collected, used, and maintained systematically by the federal government (Koontz, 2008).

The EINTEIN III Exercise PIA states however, that those sending Internet traffic to or from federal systems are not privy to a right to privacy because they have given consent. That being the case, revising of the Privacy Act's definition of Systems of Record, as suggested, would cover EINSTEIN III as it does collect PII. However, it

would not apply any greater protection to the PII because the PIA holds that consent was given. Revising the definition of a System of record does not go far enough to protect PII in the case of EINSTEIN, especially in the cases where PII is collected mistakenly.

3. Literature Ignores EINSTEIN III Legal Opinions Failure to Address the Lack of Consent

The article, *Cybersecurity and Freedom on the Internet*, (Nojeim, 2010) argues that cybersecurity policy and practices should avoid mandatory participation from private industry, because no measures are in place to prevent misuse of information. Instead of requiring the participation of private companies, the article proposes offering incentives to the private companies to encourage their sharing of threat information (Nojeim, 2010).

The article, *Square Legal Pegs in Round Cyber Holes*, (Greer, 2010) states an opposing view on the participation or private communications companies. Here the researcher suggests that it might be necessary to draft regulations making the sharing of data mandatory for owners of critical infrastructure (Greer, 2010).

Both articles failed to acknowledge the lack of consent from private communications companies' customers. The issues of voluntary or mandated private company participation can only be addressed after the issue of illegal monitoring of innocent communications without the consent is addressed.

E. SUMMARY

Before analyzing literature on the broader subject of *privacy* and *technology*, it was necessary to review the policy documents central to the research are of this thesis. Through careful examination of the *EINSTEIN III Testing Exercise Privacy Impact Assessment (PIA)*, several questions have been raised, and gaps in privacy protections discovered. By reviewing the document, the purpose of this research is better understood, and research questions validated.

Next a survey of literature about the broader subject provided an overview of significant writings within the research area. The article *Cybersecurity and Freedom on the Internet* (Nojeim, 2010) provides the most significant contribution to *privacy* and

technology understanding, as it is the one that most directly confronts privacy concerns surrounding, specifically, Cyberspace and the Internet. It directly addressed legal issues, and the participation of private ISP's in programs such as EINSEIN, and even offered solutions to protect privacy while also securing government networks.

The article *Privacy; Congress Should Consider Alternatives for Strengthening Protection of Personally Identifiable Information* (Koontz,2008) provided a greater understanding of privacy laws and guidance in regard to the collection of PII, and the article *Square Legal Pegs in Round Cyber Holes* (Greer, 2010) provided insight into possible new governance structures and/or reforming of the defined boundaries of cyberspace. Least pertinent to our understanding of *privacy* and *technology* was the thesis *Striking the Right Balance* (Skahill, 2010). Although the writing provided a framework for understanding changing policy as a means of protecting privacy rights, it was not relevant enough to this thesis's topic of research, as it deals with fusion centers collecting data and not the technology that they might use.

V. RECOMMENDED POLICY

A. A NEW EINSTEIN III PIA

1. Independent Review

In the event that collected PII is required for future analysis of a Cyber threat, the EINSTEIN III Privacy Impact Assessment (PIA) states that before that information is retained, information handling procedures have to be conducted to summarize and document why the information is necessary, and that, both the U.S. CERT Director and Deputy Director be provided weekly summaries of all instances when this is done. Further, the process is subject to periodic review by the Oversight and Compliance Offices of U.S. CERT and CS&C (Department of Homeland Security, 2010).

The fact that the periodic review is conducted within the Department of Homeland Security creates a conflict of interest. Policy regarding privacy compliance should be under the oversight of individuals that are impartial and unbiased. A group or committee with no involvement or allegiances to the DHS should conduct the periodic review to be described in a new EINSTEIN III PIA. This thesis recommends that the EINSTEIN III initiative PIA be re-written to include the creation of an independent committee to conduct, or be a party to, the weekly summaries and the periodic review process. In this way, the improper handling of PII will be less likely and conflicts of interest that may allow the misuse of PII to go unchecked will be reduced.

2. Remedial Actions

In the event that the EINSTEIN III IDS mistakenly monitors traffic that is not destined to, or originating from government computer networks, the current PIA states that the traffic will be removed and that U.S. CERT will analyze the situation and provide remedial actions. However, the PIA gives no further description of the remedial action that will be taken, nor does it describe any procedure to notify the originators of the misdirected traffic about the incident. Furthermore, the PIA does not provide redress

instructions for the originators of the misdirected traffic (Department of Homeland Security, 2010).

This thesis recommends that the EINSTEIN III initiative PIA be re-written to include a complete description of remedial actions that will be taken in the event of EINTEIN III mistakenly monitors traffic that is not destined to, or originating from government computer networks. Remedial action procedures to notify the originators of the misdirected traffic, and redress instruction might be based, in-part, on the Department of the Navy's (DON) PII breach reporting procedures.

The policy for the DON states that all commands must have designated a person in writing who is responsible for submitting DON breach reports using OPNAV 5211/13: *DON Loss or Compromise of Personally Identifiable Information (PII) Breach Reporting Form* and OPNAV 5211/14: *DON Loss or Compromise of Personally Identifiable Information (PII) After Action Reporting Form*. The procedure states that within one hour of discovery of a loss or suspected loss of PII, the designated privacy official must notify proper authorities using OPNAV form 5211/13, and that the initial report include a brief description of the incident, including circumstances of the breach, type of information lost or compromised, whether the PII was encrypted, and whether the recipients had a need to know (Schmith, 2011).

Within 24 hours of receipt, the DON CIO reviews the initial report and determines the potential risk of harm to affected personnel. Within 10 days, if required, the designated privacy official must mail notification letters to affected personnel, and within 30 days of the breach, the designated privacy official, using OPNAV form 5211/14, must send notice to the appropriate authorities of remedial actions taken to prevent recurrence, notification status, lessons learned and disciplinary action taken, where appropriate (Schmith, 2011).

3. Redactions

On March 11, 2012, EPIC requested from the Department of Homeland Security, the Privacy Impact Assessment for the pilot exercise of EINSTEIN III, as well as *all contracts with private vendors, legal opinion, security analysis, and risk assessments*

concerning the program (U.S. Department of Homeland Security, 2012). The Privacy Impact Assessment for the Initiative Three Exercise was published a week later on March 18, 2010 (Department of Homeland Security, 2010).

To date, the Department of Homeland Security has not released the full, classified PIA for the EINTEIN III in either complete or redacted form, but instead drafted a different version for release to the public. This thesis recommends that the new EINSTEIN III PIA be a full classified PIA and be released in a redacted form where necessary. Although it is likely that EPIC will appeal the redactions, and seek even more disclosure, the publication of a redacted PIA would be a good first step in assuring those concerned that PII is not being improper handled.

B. A NEW EINSTEIN III LEGAL COUNSEL OPINION

The PIA for the EINSTEIN III Exercise justifies its legality with analysis provided during the preceding EINSTEIN II Exercise (Bradbury, 2012). The U.S. Department of Justice Office of Legal Counsel's opinion titled, *Legality of Intrusion-Detection System to Protect Unclassified Computer Networks in the Executive Branch*, and *Legal Issues relating to the Testing, Use, and Deployment of an Intrusion-Detection System (EINSTEIN 2.0) to Protect Unclassified Computer Networks in the Executive Branch.* The opinion concluded that user consent is given to the monitoring of network traffic to and from government agency computer networks, by implementing and enforcing the use of model log-on banners (Bradbury, 2012). Additionally the legal opinion states that government employees give consent to the search by agreeing to a computer-users agreement that notifies them of monitoring, and that any person sending information to a government employee is not privy to a reasonable right to privacy in regard to their communications, as they, *cannot object if the third party conveys that information or records thereof to law enforcement authorities* (Bradbury, 2012).

However, the legal opinion was based on the capabilities of EINSTEIN II, which was deployed only on the networks of participant government agencies, and monitored recorded Internet traffic. EINSTEIN III, monitors traffic on live networks in real-time (Department of Homeland Security, 2010). This ability, coupled with its proposed

deployment on the network of private telecommunication providers, and the possibility of innocent Internet traffic being mistakenly monitored, makes re-using the legal bases for EINSTEIN II inappropriate as it does not address the issue of consent not being obtained by all of the customers of the participant private telecommunication providers. If PII is obtained through Internet traffic that was mistakenly monitored or prevented, the absence of consent by the private telecommunication provider's customer would, according to the EINSTEIN III PIA, be considered an illegal search based on the requirements of the Wiretap Act, FISA, and the Pen/Trap Act (Bradbury, 2012).

This thesis recommends DOJ reexamine the legal issues in the context of the new capabilities and deployment intentions of the EINSTEIN III Exercise, and that DHS include updated legal opinions in a rewritten EINSTEIN III Legal Counsel's opinions. In the drafting of a new EINSTEIN III DHS legal counsel should address directly the technologies impact on 1st, 4th and 5th amendment rights. Additionally, drafters of new legal opinion should make use of one or all of the following exemptions provided for in current communications legislation.

1. Federal Communications Act Exemption

Drafters of a new EINSTEIN III legal opinion should be able to justify the monitoring of ISP Internet traffic by invoking provisions of Section 605 of the Federal Communications Act. The Act provides for Fourth Amendment protections as it states, *No person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communications to any person* (47 U.S.C. 151, 1934). Section 605 does not restrict officials from engaging in wiretapping, it only prevents them from disclosing intercepted communications in court proceedings (Solove, 2006). In this way, drafters of a new EINSTEIN III legal opinion can justify the technologies legality by stating that no part of captured data, to include PII, would be allowed as evidence in court.

Additionally, drafters of a new EINSTEIN III legal opinion could incorporate Section 606 of the Federal Communications Act. Section 606 provides for suspension or amendment of the rules and regulations governing intercepted communications by the

President. Section 606 states that if the President proclaims that there exists a war, threat of war, state of public peril, disaster or national emergency, he may, in the interests of national security, authorize government use or control of communications facilities, and suspend or amend rules and regulations applicable to any or all stations or devices capable of emitting electromagnetic radiations (47 U.S.C. 151, 1934). Drafters of a new EINSTEIN III legal opinion should seek a pronouncement from the President that states that there indeed exists a threat of war as a result of attacks in Cyberspace, and that the use of the exemptions afforded in Section 606 of the Federal Communications Act can be applied to EINSTEIN III's monitoring of ISP networks.

However, it should be noted that even if the drafters of a new EINSTEIN III legal opinion where to incorporate these exemptions they would still be left with a problem. Although Section 605 and Section 606 offer protections to the right of due process, and a legal foundation for EINSTEIN III's monitoring of ISP network traffic, they do not prevent the solitude or privacy of those being monitored from being invaded; in other words it would not prevent *intrusion upon seclusion*.

Additionally it is likely that a presidential invocation of Section 606 exemptions would bring about heavy opposition from privacy advocates, and American citizens, who might view the application of such exemptions abusive, and overreaching in the absence of a more tangible threat to national security.

2. Title III of the Omnibus Exemption

Title III of the Omnibus Crime Control and Safe Streets Act prohibits the unauthorized, nonconsensual interception of wire, oral, or electronic communications by government agencies as well as private parties. However, the Act does provide some exceptions that could be used by the drafters of a new EINSTEIN III legal opinion.

The first exemption states that service providers may circumvent the Act's prohibitions on nonconsensual interception of wire, oral, or electronic communications, for uses *in the normal course of (their) employment while engaged in any activity which is a necessary incident to the rendition of (their) service.* Drafters of a new EINSTEIN III legal opinion could use this exemption to establish the legality of participant IPS's.

Participant ISPs could declare that the monitoring of their networks by ENSTEIN III is necessary to the rendition of their services, as they have agreed to play a role in securing government networks. Those ISP customers who do not agree to the monitoring would be free to reject the participant ISP's services and therefore be free from such monitoring.

An additional exemption to the Act states that there is an exception to the requirement that government officials obtain a warrant before intercepting covered communications where a specially designated investigative or law enforcement officer, *reasonably determines that an emergency situation exists that involves: immediate danger of death or serious physical injury to any person, conspiratorial activities threatening the national security interest, or conspiratorial activities characteristic of organized crime* (47 U.S.C. 151, 1934). Research suggests that the drafters of a new EINSTEIN III legal opinion could use this exemption to justify the legality of the technology's use. The drafters should explain in detail that the exemption applies in instances of Cybersecurity attacks on government networks as they significantly *threaten national security* by having the possible effect of disruption of service and corruption of command and control of U.S. Armed Forces and/or U.S. nuclear arsenal. Additionally the new legal opinion should explain that an attack on national infrastructure networks is especially relevant, and has the potential to result in i*mmediate danger of death or serious physical injury* as a result of a disruption, or corruption, of service to transportation, energy, or water services.

3. FISA and CyberSpace as a Foreign Domain

Another exemption that could be exploited by the drafters of a new EINSTEIN III legal opinion can be found in the Federal Intelligence Surveillance Act, or FISA. Unlike Title III of the Omnibus Crime Control and Safe Streets Act which applies to electronic surveillance for domestic law enforcement purposes, FISA is applicable when the purpose of the surveillance is to gather foreign intelligence. FISA permits electronic surveillance and covert searches pursuant to court orders issued after a review by a special court of seven federal judges, the Federal Intelligence Surveillance Court (FISC). Under FISA, orders are granted if there is probable cause to believe that the monitored

party is a *foreign power* or *an agent of a foreign power,* and there is a showing of probable cause that the surveillance will uncover evidence of criminal activity (Solove, 2006).

If Cyberspace were to be considered Foreign and attacks derived from it committed by Foreign Powers, monitoring by EINSTIEN III IDS could be seen as legal, based on FISA provisions. Drafters of a new EINSTEIN III legal opinion should seek to incorporate an administrative declaration of Cyberspace being a foreign domain, and that as such, EINSTEIN III's monitoring of network traffic be seen as legal and justified based on FISA provisions. Further if it is the intention of those administering EINSTEIN III to be able to use evidence captured as a result of EINTEIN III monitoring in court, a Federal Cyberspace Intelligence Surveillance Court (FCISC) should be established, and operated in much the same way as FISC, which permits electronic surveillance only after a review determines that there is probable cause to believe that the monitored party is a *foreign power* or *an agent of a foreign power* (Solove, 2006). FCISC, unlike FISC however, would have to make legal determination about the admissibility of cyber-attack evidence after it has already been captured and since Cyberspace will have been declared a foreign domain, a determination of whether the monitored party is a *foreign power* or *an agent of a foreign power* would not be necessary.

4. Freedom of Speech and Intrusion upon Seclusion

There are opposing arguments as to whether private ISPs should be required to participate in sharing of threat information or whether they should be incentavised to do so vountarily (Nojeim, 2010)(Greer, 2010). The issues of voluntary or mandated private company participation however, can only be addressed after the issue of illegal monitoring of innocent communications without consent is addressed; specifically, EINSTEIN III's lack of protections from intrusion upon seclusion. As defined by the *Restatement of Torts*, intrusion upon seclusion is committed by, *one who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person* (Harvard University, 2012).

Although it is unclear whether evidence obtained via EINSTEIN can be used in a trial, the technology does seem to intrude upon the seclusion, making DHS liable, even if there is no publication or other use of any kind of the information outlined (Harvard University, 2012).

To remedy EINSTEIN III's intrusion upon seclusion, drafters of a new EINTEIN legal opinion, and new privacy impact assesment, should acknowlege this limitation by establishing and publishing a procedure that ensures captured PII is never viewed by a human. Such technology should strip all private data from the offending communication and only allow the threat signature information to be used in an effort to prevent an ongoing attack. Additionally, the PII stripping process should be independently audited, and verifications published before EINTEIN III is deployed, and then again every year that it is in use. In this way intrusion upon seclusion can be prevented, and verification of its prevention made available to all EINSTEIN III participating ISP's customers.

5. The Special Needs Exemption

A report published by the Congressional Research Service (CRS) points out arguments in favor of applying the *special needs exception* to the EINSTEIN III program. The special needs exception states that, where Courts have held that *there are special governmental needs, beyond normal law enforcement*, the government may need neither a warrant nor any level of individualized suspicion. The CRS report gives as examples of such cases, the rules used to support sobriety roadblocks and border searches. The report suggests that an argument could be made that obtaining a warrant for a cyber-threat is impractical, and that since the purpose of the EINSTEIN program is beyond normal law enforcement, the application of the special needs doctrine to the EINSTEIN program may be justified (U.S. Library of Congress, 2012). This thesis supports the CRS belief that the EINSTEIN program is beyond normal law enforcement, and that the special needs doctrine does apply. Drafters of a new EINSTEIN III PIA should include an explanation of the special needs doctrine, and state specifically that, in part, this exemption provides for the legal execution of the EINSTEIN program.

C. THE SECURE IT ACT OF 2012 AND THE CYBERSECURITY ACT OF 2012

Both EPIC and CDT oppose provisions of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act (SECURE IT), and the Cybersecurity Act of 2012 that proposes exemptions for *information shared with or provided to cybersecurity centers*, as well as the proposed exemptions that would specifically exempt from disclosure all *cyber threat information* shared with the government. Opposition stems from a broadly defined *cyber threat information* that could include a large amount of information unrelated to cybersecurity (Rotenberg, McCall, & Stepanovich, 2012).

Additionally, both organizations believe that those Act's provisions governing disclosure of information to law enforcement which state that a, *cybersecurity exchange that is a Federal entity may disclose cybersecurity threat indicator* (if) *the information appears to relate to a crime which has been, is being, or is about to be committed* would, essentially, allow the government to flag any activity which may indicate a potential crime; a practice that could potentially violate search and seizure rights protected by the 4th amendment (Mills, 2012). Specifically, EPIC believes that the Acts fails to provide meaningful transparency and accountability protections, and that the handover of U.S. cybersecurity operations to the National Security Agency coupled with new exemptions from the Freedom of Information Act drastically limits public oversight necessary to prevent abuse and protect public privacy (Jackson, 2012).

CDT is also critical of the Act's FISMA reform provisions which authorizes federal agencies to share sensitive personally identifiable information (PII) with the Department of Homeland Security and also authorizes DHS to disclose that information for law enforcement purposes, and CDT believes that these provisions are specifically intended to facilitate operation of EINSTEIN (Center for Democracy & Technology, 2012a).

This thesis suggests that both the SECURE IT Act, and the Cybersecurity Act of 2012 be re-drafted, and that in those drafts the definition of *cybersecurity threat indicator*

and/or *cyber threat information* be given in a clear and understandable manner, so that proper public scrutiny and oversight can prevent abuse of discretion (Rotenberg, McCall, & Stepanovich, 2012). This thesis also suggests that the SECURE IT Act and the Cybersecurity Act of 2012 be re-drafted to remove the provision that allows non-cybersecurity information to be disclosed for law enforcement as well for *national security* purposes. Additionally the Act should include literature, that states specifically that any and all information obtained is only used for cybersecurity related issues, and that separate legislation is drafted that states specifically that the NSA be prohibited from accepting and/or soliciting Cybersecurity information form private organizations and individuals.

D. SUMMARY

Through the creation of an independent committee to conduct, or be a party to, weekly summaries and periodic reviews, the improper handling of PII would be limited. Additionally, the incorporation of remedial action procedures based on the Department of the Navy's (DON) PII breach reporting procedures, and the publication of a redacted, classified PIA, would remove many concerns about PII being improperly handled. New legal opinions, based on current EINSTEIN III program capabilities would also strengthen public belief that 1^{st,} 4th and 5th amendment rights are being protected, and the use of exemptions found in the, Federal Communications Act, Title III, and FISA can be used to form the legal basis for the employment of EINSTEIN III.

To balance between the need to collect and use information, while also preserving individual rights, privacy protection application must be consistent across all federal activities (Koontz, 2008). To accomplish this, the SECURE IT Act, and the Cybersecurity Act of 2012, should be modified to better define, *cybersecurity threat indicator* and/or *cyber threat information,* and provision within them that allows non-cybersecurity information to be disclosed for law enforcement and *national security* purposes be removed. Additionally the Acts should include literature, that states that all information obtained be used for cybersecurity related issues only, and that the NSA is prohibited from accepting and/or soliciting Cybersecurity information form private

organizations and individuals. By doing so, the Department of Homeland Security should strengthen public confidence in their ability to moderate the trade-off between defending the nation's system of computer networks, and protecting individual rights

THIS PAGE INTENTIONALLY LEFT BLANK

.

VI. SUMMARY, CONCLUSIONS, AND RECOMMENDATIONS

A. SUMMARY

Concerns surrounding the privacy implications of the EINSTEIN program, and pending legislation that appears to lay the legal groundwork for it, are well documented. Private individuals and civil rights organizations are specifically concerned with potential mistaken capture of communications, the potential misuse of personal information, and the effects of such monitoring on free speech (Center For Democracy & Technology, 2009). The theme that underpins most concerns is that the program's secrecy alone undermines the effectiveness of cybersecurity efforts, especially where the government is cooperating with private sector companies (Center For Democracy & Technology, 2009). In attempts to lift the veil of secrecey, several privacy and civil rights advocates have challenged the legitimacy of recent cybersecurity regulations and policies (Shaw, 2010).

If the policy document, *Privacy Impact Assessments for the Initiative three Exercise (EINSTEIN),* is to be improved, its drafters must address specific privacy concerns head-on. New technologies such as the EINSTEIN III IDS will, no doubt, continue to bring about questions surrounding privacy, and while it is true that no amount of research, policy or legal precedent will ever be the final answer to the question of privacy, the past must be deeply ingrained in future solutions (Solove, 2008). Incorporating answers to as many specific privacy concerns as possible is essential for public acceptance of such invasive technologies, and is what has to be done in all future policy documents surrounding the EINSTEIN III, IDS

B. CONCLUSIONS

Through in-depth analysis of existing DHS documents, *Privacy Impact Assessments for the Initiative three Exercise (Einstein)*, *Legality of Intrusion-Detection System to Protect Unclassified Computer Networks in the Executive Branch*, and *Legal Issues relating to the Testing, Use, and Deployment of an Intrusion-Detection System (EINSTEIN 2.0) to Protect Unclassified Computer Networks in the Executive Branch*, this

thesis offers strategies to address privacy concerns with the implementation of the EINSTEIN III initiative.

By reviewing current privacy policy and past privacy case studies, in addition to careful analysis of federal court cases and statutes, the fundamental and constitutional right to privacy has been established. Research has identified elements and exemptions of current communications legislation that can be used in the development of a comprehensive cyberspace monitoring policy. Recommendations have been made for the drafting of a new EINSTEIN III PIA, as well a new legal opinion that balances the trade-off between privacy rights and the objectives of securing cyberspace, and that establishes a proper legal foundation. Drafting of these policies is necessary in moving forward with the exercise, and ultimately to the implementation of the network security system. The Department of Homeland Security should follow these recommendations as a means of bolstering public confidence in their ability to moderate the trade-off between defending the nation's system of computer networks, and protecting individual rights.

C. RECOMMENDED FURTHER RESEARCH

Because the EINSTEIN program is ongoing, further research should be conducted as the program matures and evolves. Existing policies that impact privacy are updated, and new policies drafted, that ultimately alter the effects on privacy that programs like EINSTEIN have. As lawmakers work to improve the correlation between privacy laws and the expectations of the countries citizenry, so should the developers of the EINSTEIN III IDS.

The research conducted for this thesis was secondary, and was conducted through examination of EINSTEIN at the unclassified level. Further research should include primary research, in which the opinions of those opposed to the EINSTEIN III IDS are collected via interviews and/or questionnaires. Additionally the developers of the technology, and more importantly the writers of the technologies' privacy oriented policies, should be interviewed to better understand the reasoning behind some of the important decisions pointed out in this thesis, such as the re-use of the EINSTEIN II Legal Opinion, and the lack of redress and remediation procedures. It is possible that

many of the decisions surrounding the EINSTEIN program were made as a result of the necessarily secretive nature of the technology, and that further research conducted at a security level high enough to allow for candid and comprehensive responses to research questions might reveal relevant information regarding the EINSTEIN program.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Administrative Office of the U.S. Courts. (2012, November 2). *Precedents*. Retrieved from http://www.uscourts.gov/EducationalResources/ConstitutionResources/SupremeCourtDialogs/JudicialInterpretationDiscussionTopics/Precedents.aspx

American Civil Liberties Union. (2012, September 28). *EINSTEIN's threat to online privacy?* Retrieved from https://www.aclunc.org/issues/technology/blog/einstein%27s_threat_to_online_privacy.shtml

American Civil Liberties Union. (2009, November 17). *Doe v. Holder : Internet service provider's NSL*. Retrieved from http://www.aclu.org/national-security/doe-v-holder

Bradbury, S. G. (2009, January 9). *Legal issues relating to the testing, use, and deployment of Einstein 2.0.* Retrieved from Justice.gov: http://www.justice.gov/olc/2009/e2-issues.pdf

Brown, P., & Williams, A. (2012, November 2). *Introduction to legal research*. Retrieved from GSU Law Library website: http://libguides.law.gsu.edu/content.php?pid=154797&sid=1312326

Caplan, R. L. (1983, March). The history and meaning of the Ninth Amendment. *Virginia Law Review*, 69, 223–268. Retrieved from http://www.jstor.org/stable/1072779

Center For Democracy & Technology. (2009). *Einstein intrusion detection system: Questions that should be addressed.* Washington, DC. Retrieved from https://www.cdt.org/security/20090728_einstein_rpt.pdf

Center for Democracy & Technology. (2012, September 28). *About CDT*. Retrieved from CDT website: https://www.cdt.org/about

Center for Democracy & Technology. (2012a). *Information sharing, monitoring, and countermeasures in the Cybersecurity Act, S. 2105, and the SECURE IT Act, S. 2151.* Retrieved from https://www.cdt.org/files/pdfs/analysis_senate_cyberbills_2012.pdf

Chertoff, M. (2008, April). Remarks by Homeland Security Secretary Michael Chertoffto the 2008 RSA conference, San Francisco, CA. Retrieved fom http://www.hsdl.org/?view&did=486710

Coldabella, G. P., & White, B. M. (2010). Foundational questions regarding the Federal role in cyberspace. *Journal of National Security Law & Policy*, 233–245. Retrieved from http://insct.org/jnslp/wp-content/uploads/2010/08/15_Coldebella-White.pdf

Computer Matching and Privacy Protection Act of 1988, 54 FR 25818, (1988). Retrieved from http://www.privacilla.org/government/cmppa.html

Communications Act of 1934, 47 U.S.C. 151. (1934) Retrieved from Justice Information Sharing website: http://www.it.ojp.gov/default.aspx?area=privacy&page=1288#contentTop

Couch v. United States, 409 U.S. 322 (1973). Retrieved from http://supreme.justia.com/cases/federal/us/409/322/

Culotta, M. L., & Fredrickson, A. J. (2007). Holes in the fence: Immigration reform and border security in The United States. *American Bar Association, Administrative Law Review,* 59, 521-532. Retrieved from http://web.ebscohost.com.libproxy.nps.edu/ehost/detail?sid=e0c4f73a-0514-43e6-96ff-cd27c933c937%40sessionmgr104&vid=2&hid=112&bdata=JnNpdGU9ZWhvc3QtbGl2ZSZzY29wZT1zaXRl#db=bth&AN=26818786

Cybersecurity Act of 2012, S. 2105 (2012). Retrieved from http://www.govtrack.us/congress/bills/112/s2105/text

Dasgupta, P., Chatha, K., & Gupta, S. K. (2007). *Viral attacks on the DOD Common Access Card (CAC).* Tempe, AZ: Arizona State University. Retrieved from http://cactus.eas.asu.edu/partha/papers-pdf/2007/milcom.pdf

DeCew, J. (2008). *Privacy.* The Stanford Encyclopedia of Philosoph. Retrieved from http://plato.stanford.edu/archives/fall2008/entries/privacy/

Desai, A. C. (2007). Wiretapping before the wires: The post office and the birth of communications privacy. *Stanford Law Review*, 60, 553–594. Retrieved from http://legalworkshop.org/wp-content/uploads/2009/04/stan-a-0005-desai.pdf

Doe v. Gonzales, 546 U. S. ____ (2005). Retrieved from http://www.supremecourt.gov/opinions/05pdf/05a295.pdf

Doe v. Holder, 04 Civ 2614 (2009, August 5). Retrieved from http://www.aclu.org/files/pdfs/safefree/doevholder_amendedredacteddecl_08052009.pdf

Doe v. Holder, 04 Civ 2614 (2010, March 18). Retrieved from http://www.aclu.org/files/assets/Marrero_Decision_and_Order.031810.pdf

Dondershine, H. (2012, July 06). *Substantive due process* . Retrieved from http://www.stanford.edu/group/psylawseminar/Substantive%20Due%20Process.htm

Duke Law Journal. (1973). Developments under the Freedom of Information Act: 1972. *Duke Law Journal*, 157, 178–206. Retrieved from http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=2432&context=dlj

Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. 2510–22. (1986). Retrieved http://www.it.ojp.gov/default.aspx?area=privacy&page=1285#contentTop

Electronic Privacy Information Center. (2012, August 14). *The Privacy Act of 1974*. Retrieved from http://epic.org/privacy/1974act/

EPIC vs. NSA, Civil Case 10–1533 (2011, July 8). Retrieved from http://epic.org/privacy/nsa/foia/EPIC-v-NSA-Order.pdf

EPIC vs. NSA, Appeal, 11–5233 (2012, May 11). Retrieved from http://www.cadc.uscourts.gov/internet/opinions.nsf/2772CC6C7E277C1C852579FB004DB101/$file/11-5233-1373260.pdf

Foxman, E. R., & Kilcoyne, P. (1993). Information technology, marketing practice, and consumer privacy: Ethical issues. *Journal of Public Policy & Marketing*, 12–1, 106–119. Retrieved from http://www.jstor.org/stable/30000116

Froomkin, A. M. (2007). Creating a viral federal privacy standard. *Boston College Law Review*, 48, 55–120. Retrieved from http://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=2346&context=bclr

Freedom of Information Act of 1966, 5 U.S.C. 552, (1966). Retrieved from http://www.justice.gov/oip/foia_updates/Vol_XVII_4/page2.htm

Goldsmith, J. (2010, December 08). *The cyberthreat,government network operations, and the Fourth Amendment.* Retrieved from Brookings website: http://www.brookings.edu/~/media/research/files/papers/2010/12/08%204th%20amendment%20goldsmith/1208_4th_amendment_goldsmith.pdf

Govindaiah, M. (2006). Driver licensing under the real id act: can current technology balance security and privacy? *Journal of Law, Technology & Policy*, 2006, 201–213. Retrieved from http://www.jltp.illinois.edu/recdevs/govindaiah.pdf

Greer, J. N. (2010). Square legal pegs in round cyber holes: The NSA, lawfulness, and the protection of privacy rights and civil liberties in cyberspace. *Journal of National Security Law & Policy*, 4, 139–154. Retrieved from: http://jnslp.com/wp-content/uploads/2010/08/10_Greer.pdf

Harvard University. (2012, June 27). *Restatement of the law, second, torts*, 652. Retrieved from http://cyber.law.harvard.edu/privacy/Privacy_R2d_Torts_Sections.htm

Hill, G., & Hill, K. (2012, November 2). *Stare decisis*. Retrieved from Legal Dictionary website: http://dictionary.law.com/Default.aspx?selected=2005

Jackson, W. (2012, July 02). *McCain's retooled Secure IT act still a privacy threat, critics say*. Retrieved from Government Computer News website: http://gcn.com/articles/2012/07/02/secure-it-act-amended-critics-say-still-threat-to-privacy.aspx

Jansen, J. (2006, May 24). *Federal court rules permanent ban on NSL speech may infringe First Amendment*. Retrieved from Jurist website: http://jurist.law.pitt.edu/paperchase/2006/05/federal-court-rules-permanent-ban-on.php

Karger, P. A. (2006). Privacy and security threat analysis of the federal employee Personal Identity Verification (PIV) Program. *IBM Research Division, Thomas J. Watson Research Center*. Retrieved from http://cups.cs.cmu.edu/soups/2006/proceedings/p114_karger.pdf

Katz v. United States, 389 U.S. 347 (1967). Retrieved from http://www.oyez.org/cases/1960–1969/1967/1967_35

Koontz, L. (2008). *PRIVACY: Congress should consider alternatives for strengthening protection of personally identifiable information* (GAO-08-795T). Washington, D.C.: Governement Accountability Office. Retrieved from http://www.gao.gov/new.items/d08795t.pdf

Kozel, R. (2010). *Stare decisis as judicial doctrine.* Washington and Lee Law review, 67, 410-466. Retrieved from http://scholarlycommons.law.wlu.edu/wlulr/vol67/iss2/2

Lane, F. S. (2009). *American privacy: The 400-year history of our most contested right.* Boston, MA: Beacon Press.

McCullagh, D. (2012, April 24). *CISPA revision allows DHS Internet 'countermeasures'*. Retrieved from CNET News website: http://news.cnet.com/8301-31921_3-57420580-281/cispa-revision-allows-dhs-internet-countermeasures/

McLaughlin, E. C. (2007, August 16). *Federal ID plan raises privacy concerns.* Retrieved from CNN.com website: http://www.cnn.com/2007/POLITICS/08/16/real.id/

Mills, E. (2012, February 23). *Civil liberties groups: Proposed cybersecurity bill is too broad*. Retrieved from CNET News website: http://news.cnet.com/8301-27080_3-57384137-245/civil-liberties-groups-proposed-cybersecurity-bill-is-too-broad/

Nakashima, E. (2009, July 3). Cybersecurity plan to involve NSA, telecoms. *The Washington Post*. Retrieved from http://articles.washingtonpost.com/2009-07-03/news/36822001_1_networks-einstein-obama-administration

National Security Council. (2012, September 24). *The comprehensive national cybersecurity initiative.* Retrieved from The White House website: http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative

Nieland, A. E. (2007). National security letters and the amended Patriot Act. *The Cornell Law Review*,92, 1201–1238. Retrieved from http://www.lawschool.cornell.edu/research/cornell-law-review/upload/Nieland.pdf

Nojeim, G. T. (2009). *Cybersecurity:Preventing terrorist attacks and protecting privacy in yberspace.* Retrieved from CDT website: https://www.cdt.org/testimony/gregory-t-nojeim-cybersecurity-preventing-terrorist-attacks-and-protecting-privacy-cybersp

Nojeim, G. T. (2010). Cybersecurity and freedom on the Internet. *Journal of National Security Law & Policy*, 119–137. Retrieved from http://jnslp.com/wp-content/uploads/2010/08/09_Nojeim.pdf

Olmstead v. United States, 277 U.S. 438 (1928). Retrieved from http://www.oyez.org/cases/1901–1939/1927/1927_493

Privacy Act of 1974, 5 U.S.C. § 552a. (1974). Retrieved from http://www.justice.gov/opcl/privstat.htm

Prosser, W. (1960). Privacy. *The California Law Review*, 48, 383-423. Retrieved from http://www.californialawreview.org/assets/pdfs/misc/prosser_privacy.pdf

Planning for the Future of Cyber Attack Attribution: Hearing Before the H. Subcomm. on Technology and Innovation of the H. Comm. on Science and Technology, 111th Cong., (2010) (testimony of Marc Rotenberg/EPIC). Retrieved from http://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=1106&context=cong

Rotenberg, M., McCall, G., & Stepanovich, A. (2012). *FOIA: Safeguarding critical infrastructure: Statement by EPIC.* Washington, DC: Electronic Privacy Information Center (EPIC). Retrieved from http://www.judiciary.senate.gov/resources/transcripts/upload/031312RecordSubmission-Leahy.pdf

Schmith, M. (2011, July). *Report your breaches*. Retrieved from *CHIPS website: http://www.doncio.navy.mil/CHIPS/ArticleDetails.aspx?id=2494*

Schneider, C. E. (1988). State-Interest analysis in Fourteenth Amendment "privacy" law. *Law and Contemporary Problems*, 59, 79-122. Retrieved from http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=3937&context=lcp

Seipp, D. J. (1978). *The right to privacy in American history*. Cambridge, MA: Harvard University Press.

Shaw, J. A. (2010). *The right to privacy and cybersecurity: Safeguarding american values.* (Master's thesis, Georgtown Univeristy). Retrieved from http://repository.library.georgetown.edu/bitstream/handle/10822/553583/shawJames.pdf?sequence=1

Skahill, T. M. (2010). *Striking the right balance: Fusion centers and privacy.* (Master's thesis, Naval Postgraduate School).Retrieved from http://edocs.nps.edu/npspubs/scholarly/theses/2010/Sep/10Sep_Skahill.pdf

Smith, J. E. (2007). You can run, but you can't hide: Protecting privacy from radio frequency. *North Carolina Journal of Law & Technology*, 8, 249–272. Retrieved from http://www.ncjolt.org/sites/default/files/249-272_smith-vol8iss2.pdf

Smith v. Maryland, 442 U.S. 735 (1979). Retrieved from http://supreme.justia.com/cases/federal/us/442/735/case.html

Solove, D.J. (2004). The digital person. New York, NY: New York university Press.

Solove, D. J. (2006). A brief history of information privacy law. *Proskauer on Privacy*,

Solove, D. J. (2008). Understanding privacy. Cambridge Massachusetts: Harvard University Press.

Solove, D. J. (2010). Fourth Amendment pragmatism. *Boston College Law Review*, 51, 1511-1538. Retrieved from http://www.bc.edu/content/dam/files/schools/law/bclawreview/pdf/51_5/04_solove.pdf

The Revolutionary War and Beyond. (2012, November 2). *The 1st Amendment*. Retrieved from: http://www.revolutionary-war-and-beyond.com/1st-amendment.html

The President of the United States (2004, August 27). Homeland Security Presidential Directive 12. Washington, DC: George W. Bush. Retrieved from http://www.dhs.gov/homeland-security-presidential-directive-12

Title III of the Omnibus Crime and Safe Streets Act of 1968 (Wiretap Act), 42 U.S.C.3789d. (1968), Retrieved from http://www.it.ojp.gov/default.aspx?area=privacy&page=124#contenttop

Uniting and Strengthening America by Providing Appropriate Tools Required To Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, H.R. 3162, 107th Cong., 1st Sess. (2001).

U.S. Computer and Emergency Response Team. (2012). (2012, January 10). *About Us*. Retrieved from: http://www.us-cert.gov/about-us/

U.S. Const. amend. I.

U.S. Const. amend. III.

U.S. Const. amend. IV.

U.S. Const. amend. IX.

U.S. Const. amend. V.

U.S. Const. amend. XIV.

U.S. Department of Homeland Security (US-CERT). (2004, September). *Privacy impact assessment, EINSTEIN program, collecting, analyzing, and sharing computer security information across the federal civilian government*. Washington, DC. Retrieved from http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_eisntein.pdf

U.S. Department of Homeland Security (US-CERT). (2008, May, 19). *Privacy impact assessment for EINSTEIN 2.* Washington, D.C. Retrieved from http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_einstein2.pdf

U.S. Department of Homeland Security (US-CERT). (2010, March, 18). *Privacy impact assessment for the initiative three exercise.* Washington, D.C. Retrieved from http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_nppd_initiative3exercise.pdf

U.S. Department of Homeland Security. (2010a). *Computer network security & privacy protection.* Washington, D.C. Retrieved from http://www.dhs.gov/xlibrary/assets/privacy/privacy_cybersecurity_white_paper.pdf

U.S. Department of Homeland Security. (2012, September 24). *FOIA request log FY10* Retrieved from www.dhs.gov/xlibrary/assets/foia/priv-foia-logs-fy-2010.pdf

U.S. Department of Justice. (2012, June 25). *Highlights of the USA PATRIOT Act*. Retrieved from Justice.gov website: http://www.justice.gov/archive/ll/highlights.htm

U.S. Library of Congress, Congressional Research Service. (2002). the USA PATRIOT Act: A sketch by Charles Doyle (*CRS Report No.* RS21203). Washington, DC: Office of Congressional Information and publishing. Retrieved from http://www.fas.org/irp/crs/RS21203.pdf

U.S. Library of Congress, Congressional Research Service. (2012).). *Cybersecurity: Selected legal issues* (*CRS Report No.* R42409). Washington, DC: Office of Congressional Information and publishing. Retrieved from http://www.fas.org/sgp/crs/misc/R42409.pdf

U.S. Senate Commitee on Homeland Security & Governmental Affairs. (2012, September 24). *Cybersecurity*. Retrieved from senate.gov website: http://www.hsgac.senate.gov/issues/cybersecurity

U.S. Senate Commitee on Energy & Natural Resources. (2012, March 1). *Senators introduce legislation to strengthen cybersecurity*. Retrieved from http://www.energy.senate.gov/public/index.cfm/2012/3/senators-introduce-legislation-to-strengthen-cybersecurity

University of Miami. (2012, Jun 25). *Cable Communications Policy Act of 1984*. Retrieved from Miller School of Medicine, Privacy Data Protection Project website: http://privacy.med.miami.edu/glossary/xd_ccpa.htm

Why isn't the Department Of Homeland Security meeing the President's standard on FOIA: Hearing before the Committee on Oversight and Government Reform, 112th Cong. 1 (2011) (testimony of John Verdi/EPIC). Retrieved from http://www.hsdl.org/?view&did=7311

Zetter, K. (2010, August 10). *'John Doe' who fought FBI spying freed from gag order after 6 years*. Retrieved from Wired website: http://www.wired.com/threatlevel/2010/08/nsl-gag-order-lifted/#ixzz0wcPM40Dg

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. D. C. Boger
   Naval Postgraduate School
   Monterey, California

4. G. R. Cook
   Naval Postgraduate School
   Monterey, California

5. J. D. Fulp
   Naval Postgraduate School
   Monterey, California

6. W. L. Oree
   Naval Postgraduate School
   Monterey, California